ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
PROVOZNĚ EKONOMICKÁ FAKULTA

DISERTAČNÍ PRÁCE

HODNOCENÍ BEZPEČNOSTI INFORMACÍ V INFORMAČNÍCH SYSTÉMECH

EVALUATION OF INFORMATION SECURITY IN INFORMATION SYSTEMS

Autor: **Ing. Jiří Urbanec**
Školitel: **doc. Ing. Prokop Toman, CSc.**
Obor: **Informační management**

Praha 2015

ABSTRAKT

Informace jsou pro organizace cenným aktivem a zdrojem konkurenční výhody. Proto je nezbytné zajistit a udržovat bezpečnostní charakteristiky procesů a systémů v požadovaných mezích a průběžně kvantitativně hodnotit stav na bázi měření. Problémem při samotném procesu měření se ukazuje výběr vhodných charakteristik a měr procesů a produktů, které by byly předmětem měření. Hlavním cílem disertační práce je návrh metodiky pro hodnocení bezpečnosti informací v informačních systémech organizací měřením a formulovat závěry a doporučení pro její využití v praxi. Situace v Českých organizacích byla zjištěna na základě kvantitativního průzkumu, ve kterém byla data sbírána pomocí dotazníkového šetření (N=785, n=101) a následný kvalitativní výzkum proběhl ve 3 organizacích z finančního sektoru v České republice. Výsledky ukázaly, že v současné době nadpoloviční většina zkoumaných organizací hodnotí informační systémy z pohledu rizika pro hodnotné informace (58,49 %). Organizace, které bezpečnost informací hodnotí, tak provádějí nejčastěji s cílem identifikovat slabiny a vznikající problémy (41,5 %). Pouze 17,6 % organizací hodnotí bezpečnost informací měřením. Práce identifikuje model chování organizace, navržený metodický postup definuje vlastní měřitelné charakteristiky systému identifikované pomocí rozšířeného bezpečnostního modelu, definuje proces vývoje měr v organizaci na bázi nástroje GQM, navrhuje měření kompatibilní s ISO 27004 a prezentuje hodnocení výsledků na základě změřených výstupů. Navržené postupy a konstrukty se zaměřily na zlepšení výzkumem identifikované oblasti „klasifikace informací“ a „rozdílné vnímání hodnoty informace vlastníkem a zpracovatelem“. Ověřeny byly na dvou anonymních organizacích a jsou prezentovány ve formě případové studie. Jedním ze závěrů je, že navržená metodika je použitelná organizacemi se silným technickým a finančním zázemím, kde je možno překonat náročné požadavky procesu vývoje měr a aplikace měření. Metodika samotná má pak své vlastní limity pro aplikaci.

Klíčová slova:
Bezpečnost informací, informační systém, informace, metodika, GQM, výzkum, organizace, model, případová studie

JEL klasifikace: D82, L86

ABSTRACT

Information is a valuable asset for organizations and a source of competitive advantage nowadays. Therefore it is necessary to retain information security characteristics of processes and systems in required limits and continuously evaluate the state using measurement. The problem in measurement shows to be in the selection of suitable characteristics and measures of the processes or the products, which are subject to measurement.The main aim of the dissertation thesis is to design methodics for evaluating information security in information systems and formulate conclusions and recommendations for its use in practice. The situation in The Czech Republic was obtained based on a quantitative survey in which data was collected by means of a questionnaire survey (N=785; n=101) and qualitative research was conducted in the 3 organizastions from financial sector in the Czech Republic. Results showed that at present an absolute majority of surveyed organizations evaluate information systems from the perspective of risk to valuable information (58.49%). Organizations evaluating information security are most often to identify weaknesses and emerging issues (41.5%). Only a 17.6% of them measure. The designed methodics identifies behavioral model of the organization, defines measurable characteristics of the system and the organization based on extended security model, defines process of development of the measures based on GQM tool, engages measurement process compatible with ISO 27004 and presents evaluation procedure using measured values. The proposed procedures and constructs focused on improvement of field detected by the survey, the “information classification” and “diference between perception of information value between owner and processor”. The procedures were validated on two anonymous organisations and are presented in form of case studies. One of the conclusions is, that proposed methodics is applicable mostly in organisations with strong technical and financial base, where it is possible to overcome requirements of measures development processes and measurement application. Also the methodics of evaluation has its own limits of applicability.

Key words:

Information security, information system, information, methodics, GQM, survey, model, organization, case study

JEL classification: D82, L86

OBSAH

1 ÚVOD

V informační a znalostní ekonomice mají informace pro organizace vysokou důležitost a jsou považovány za aktiva a zdroj konkurenční výhody. Je všeobecně akceptovaným faktem, že je nutné tato aktiva v informačních systémech efektivně a bezpečně zpracovávat a eliminovat tak hrozby, které na informace působí v rámci informačního procesu. Ochranou informací se zabývá obor informační bezpečnost a obor řízení informační bezpečnosti. Cílem informační bezpečnosti je zajištění kritických charakteristik informací pro udržení kvality rozhodovacích a řídících procesů na těchto informacích závislých, zajištění soukromí osob a pokrytí legislativních požadavků. Zajištění kritických charakteristik informací lze chápat jako produkt procesů řízení informační bezpečnosti na všech úrovních řízení realizovaný prostřednictvím konkrétních opatření.

Řízení informační bezpečnosti využívají v současné době všechny organizace bez ohledu na velikost či obor činnosti, pro které jsou informace a informační technologie klíčovou součástí podnikatelských procesů, nebo které spravují citlivé informace svých klientů a mají potřebu efektivně a komplexně zajistit jejich bezpečnost. Postupy pro řízení informační bezpečnosti využívají efektivní dokumentované systémy řízení a správy informačních aktiv s cílem snížit informační rizika. Míra aplikace pravidel informační bezpečnosti a využití systémů řízení informačních rizik v informačních a komunikačních technologiích postupně roste.

Bezpečnost informací je aktuální problémová oblast na všech úrovních řízení organizace. Mezi hlavní důvody, které dokládají její význam v informačních procesech, lze uvést:

- závislost na informacích a informačních systémech vede k zachování konkurenční výhody, ziskovosti a obchodního image,
- soustavný dohled nad dodržováním legislativních, normativních a smluvně dojednaných požadavků týkajících se informací,
- potřeba ujištění zainteresovaných stran jako jsou akcionáři, klienti, odběratelé a dodavatelé, že bezpečnost informací je řízena,

- pomocí správně vyhodnocených rizik se stanoví ohrožení aktiv a je vyhodnocena zranitelnost a pravděpodobnost výskytu rizik a možné dopady tak, aby organizační zdroje byly efektivně využity (Bureau Veritas, 2010).

Disciplína informační bezpečnosti je po desítkách let vývoje v pokročilém stádiu, je teoreticky zvládnutá a v organizacích systematicky aplikována, spravována a řízena. Zásadní problematickou oblastí však zůstává schopnost přesvědčit zainteresované strany o výsledku dosahování úrovně bezpečnosti informací v informačních systémech a odpovědět na otázku úrovně kvality řízení informačních rizik v dané organizaci. Dále je řešena otázka úrovně vyspělosti procesů informační bezpečnosti a účinnosti prosazování bezpečnostních opatření, to vše v rámci komplexní organizační struktury a v neustále se měnícím se technologickém a personálním prostředí (Doucek et al., 2011, s. 37). V souvislosti s řídícími procesy v organizaci a úrovní bezpečnosti informací je vyžadováno exaktní zhodnocení pro určování organizačních priorit.

Historicky existuje množství modelů, metodik, standardů a norem, které řeší postupy a přístupy k identifikaci a řízení rizik související s informacemi jako aktivem. Dokladem jsou souhrny uváděné v Doucek (2011, s. 55-78), Whitman (2010, s. 211-242). Existující standardy rodiny ISO 27000, ISO/IEC 13335, NIST SP 800 a další normy pro řízení bezpečnosti informací mají za cíl definovat procesy a pravidla, jak dosáhnout „bezpečného systému v daném okolí“ a jsou postaveny na principu aplikace souboru účinných opatření.

Přesné absolutní resp. relativní opakovatelné měření bezpečnostní pozice informačního systému z pohledu informací využívající vhodně navržený systém měr může být použito jako důkaz dosažení konkrétní úrovně bezpečnosti informací v informačním systému. Problémovou oblastí je stanovení systému měr, který by byl kontinuálně použitelný v současných informačně vzájemně provázaných organizačních procesech, různých přístupech organizací k rizikům a globálně propojených informačních systémech. Hodnocení na základě měření není ve stávající praxi oboru informační bezpečnosti absolutní prioritou (Doucek, 2011, s. 112). Potvrzují to i aktuální výsledky v práci prezentovaného primárního výzkumu v organizacích v České

republice, postupný rozvoj aplikace standardu ISO 27004 (první i současná verze) a doposud neustálená taxonomie měr.

Pro pokrytí problémové oblasti je na základě výstupů disertační práce navržena metodika pro stanovení systému bezpečnostních měr na bázi konceptuálního nástroje GQM (Goal-Question-Metric). Míry jsou použity v modelu chování konkrétních českých organizací a je navržen způsob prezentace bezpečnostní pozice informačního systému využívající hodnot poskytnutých těmito mírami.

2 CÍL DISERTAČNÍ PRÁCE

Hlavní výzkumná otázka v disertační práci zní: jak stanovit vhodné charakteristiky a atributy informačního systému a jak identifikovat míry pro hodnocení informačního systému z pohledu zachování kritických bezpečnostních charakteristik informací?

Hlavním cílem disertační práce je návrh metodiky pro hodnocení bezpečnosti informací zpracovávaných v informačním systému a formulace závěrů a doporučení pro její využití v praxi. Praktickým přínosem práce je využití jejích závěrů ke snížení bezpečnostních rizik souvisejících s informacemi v informačních systémech organizací. Detekce odchylek a zaměření se na konkrétní slábnoucí oblasti umožní minimalizaci rizik působících na informace v informačních systémech (např. zneužití osobních, obchodních a strategických informací, intelektuálního vlastnictví apod.). Pomocí identifikovaných měr a jejich použití při stanovení tzv. bezpečnostní pozice informačního systému a v procesu auditu lze přispět k vyšší kvalitě ochrany informací a tím přispět ke zvyšování jistoty při správě a řízení investic do bezpečnosti informací. Systematizací hodnocení pozice informačního systému měřením lze dosáhnout opakované použitelnosti systému měr a vytvořit tak základ obchodního modelu Security-As-A-Service.

Formulované cíle vyplynuly z průzkumu teoretických východisek v problematice zajišťování bezpečnosti informací v informačních systémech organizací a z požadavků praxe na aplikaci metodiky hodnocení informačních systémů měřením v modelech řízení informační bezpečnosti.

Dílčí cíle práce jsou:

- identifikovat aktuální stav hodnocení bezpečnosti informací v organizacích v České republice realizací a vyhodnocením primárního výzkumu (kvantitativní a kvalitativní),
- charakterizovat míry pro hodnocení bezpečnosti informací,
- navrhnout a popsat vlastní metodiku pro identifikaci měr a prezentaci bezpečnostní pozice informačního systému,

- validovat navržený postup v konkrétní organizaci na stanovených reálných informačních systémech,
- zhodnotit vhodnost metodiky pro účely řízení informační bezpečnosti.

S ohledem na teoretická východiska disertační práce, která vyplynula z analýzy současného stavu problematiky, byly stanoveny hlavní statistické hypotézy, které budou ověřeny v rámci praktické části disertační práce kvantitativním výzkumem (budou zkoumány závislosti mezi sledovanými kvalitativními proměnnými, tj. jednotlivé otázky dotazníku s identifikačními otázkami zaměřenými na odvětví, velikost, vlastnický podíl apod.):

Hypotéza 1: V organizacích v ČR zpracovávajících hodnotné informace nejsou aplikovány postupy, standardy a normy řízení informační bezpečnosti na bázi mezinárodních ani harmonizovaných českých standardů. Hypotéza bude akceptována, pokud více než 75 % organizací neaplikuje postupy, standardy ani normy řízení informační bezpečnosti.

Hypotéza 2: Organizace v ČR zpracovávající hodnotné informace nestanovují priority cílů[1] (nehodnotí cíle shodně) v oblasti bezpečnosti informací. Hypotéza bude akceptována, pokud méně než 50 % organizací stanoví důležitost bezpečnostních cílů odlišně.

Hypotéza 3: Kvantitativní přístup k hodnocení bezpečnosti informací v organizacích v ČR zpracovávajících hodnotné informace není aplikován. Hypotéza bude akceptována, pokud více než 75 % organizací neaplikuje měření, resp. kvantitativní hodnocení bezpečnosti informací v informačním systému.

Hypotéza 4: Předpokládá se, že vlivné faktory na dosažení maximální úrovně bezpečnosti informací považuje za důležité většina organizací. Hypotéza bude akceptována, pokud každý faktor bude uveden více než u 50 % organizací.

[1] Stanovení priorit = ohodnocení důležitosti organizačních cílů v konkrétní organizaci při dosahování bezpečnosti informací (1= zcela nedůležitá, 5= velmi důležitá, je možné přiřadit stejnou důležitost). V případě, že organizace stanoví u všech cílů stejnou důležitost (např. u všech hodnotu 5= velmi důležitá), jedná se o nestanovení priorit. V případě, že alespoň u jednoho cíle stanoví organizace důležitost jinou než u ostatních, jedná se o stanovení priorit cílů.

Dále byly stanoveny výzkumné otázky, které budou ověřeny kvalitativním výzkumem (rozhovory a případovými studiemi):

Výzkumná otázka 1: Může být bezpečnost informací vyjádřena systémem měr podle navržených kritérií?

Výzkumná otázka 2: Poskytují navržené kvantitativní míry přesné informace o úrovni bezpečnosti informací v informačním systému?

Výzkumná otázka 3: Lze navržený metodický postup využít ke kvantitativnímu zhodnocení bezpečnosti informací v informačním systému?

3 METODICKÝ POSTUP

V této kapitole jsou uvedeny teoretické předpoklady využití metodického aparátu disertační práce a návrh metodiky, která byla využita při zpracování teoretické i praktické části disertační práce.

3. 1 Aplikovaný metodický aparát

Metodologie - v širším slova smyslu označuje obecná filozofická východiska vědeckého poznání, společná všem vědním disciplínám. V užším smyslu se tímto pojmem označuje teorie vědeckého poznání, která studuje procesy poznávání a přetváření skutečnosti, jež jsou předmětem konkrétních vědeckých disciplín.

Metodika – nepatří do oblasti metodologie. Metodiku výzkumné práce lze považovat za praktický postup pro praktickou postupnou realizaci výzkumné procedury vztahující se k realizaci výzkumného cíle. Tento postup lze formálně ztvárnit např. ve vývojovém diagramu či v jiném formalizovaném schématu. Jedná se o promyšlený postup činnosti k dosažení vytýčeného cíle při realizaci daného úkolu neboli uspořádaná množina činností na sebe určitým způsobem navazující. Metodický postup práce je uveden v kapitole 3 a podrobná metodika je uvedena v kapitole 3. 2.

Metoda - vědeckou metodu lze obecně charakterizovat jako záměrný postup, jehož pomocí lze dosáhnout určitého cíle. Metoda představuje obvykle celý komplex různorodých poznávacích postupů a praktických operací, které směřují k získávání vědeckých poznatků. Použití metody při vědeckém zkoumání předpokládá znát postup, jak metodu použít (Hendl, 2012, s. 321). Tento pojem je užíván v různé šíři. Nejčastěji se tímto pojmem označují speciální postupy vědní disciplíny, např. v psychologii, experimentální metoda, vědecké pozorování apod. Někdy se užívá metoda v širokém smyslu, např. metoda teoretické analýzy. Bývá pak výrazem pro označení určitého obecného poznávacího postupu, způsobu zkoumání, zahrnuje i ostatní logické prostředky (syntézu, abstrakci, zobecňování). Použité metody v rámci disertační práce jsou uvedeny v kapitole 3. 2.

Procedura - organizační uspořádání poznávacího procesu (statistická, monografická, typologická, experimentální, historická). Použité procedury jsou specifikovány v kapitole 3. 2.

Technika - vyjadřuje dílčí operace procedury. Rozlišují se techniky výběru (náhodný výběr (losování), záměrný výběr (předvýzkum), smíšený výběr (kombinace) a technika zpracování dat (kvantitativní či kvalitativní). Použité techniky výběru respondentů včetně technik zpracování dat jsou uvedeny rovněž v kapitole 3. 2.

Faktor - lze konstruovat dle prokazatelných metodických postupů a statistických analýz (Disman, 2008; Hebák, 2005). Díky konstrukci faktorů lze snadněji stanovit závěry a doporučení pro aplikování metodiky hodnocení informačních systémů z pohledu bezpečnosti zpracovávaných informací (viz kapitola 2.10).

Konstrukt - je předmět poznávání, který není přímo pozorovatelný, ale na jehož podstatu lze usuzovat na základě literárních východisek prostřednictvím vymezených vlastností a vztahů mezi nimi (Anderson, 2009). Faktory konstruktu jsou podrobovány rozboru, u kterého se využívají matematicko-statistické metody. Na základě diskutovaných faktorů ovlivňujících bezpečnost informací budou jednotlivé faktory reflektovány do dotazníkového šetření tak, aby otázky v dotazníku umožnily upřesnit platnost naměřených výsledků (tj. průkaznost faktorů a stanoveného konstruktu). Tabulka 6 (kapitola 5. 1) uvádí a specifikuje faktory ovlivňující bezpečnost informací v organizacích. Ty jsou sestavené na základě dedukovaných poznatků z literárních východisek práce. Pomocí kvantitativního výzkumu bude zjišťován vliv těchto faktorů na bezpečnost informací.

K vypracování disertační práce byly použity metody teoretické, empirické a srovnávací podle Skalkové a kol. (1983).

Z teoretických metod byla při zpracování disertační práce použita:

- analýza (rozbor vlastností, vztahů, faktů postupujících od celku k části – bylo použito např. u analýzy sekundárních zdrojů (literárních východisek práce) a identifikace faktorů ovlivňující bezpečnost informací),
- syntéza (postup od části k celku, spojení poznatků získaných analytickým přístupem, bude využito při vyhodnocování získaných primárních dat),

- indukce (vyvozování obecného závěru na základě poznatků o jednotlivostech),
- dedukce (vyvozování nových závěrů),
- abstrakce (oddělení podstatných charakteristik objektu od nepodstatných),
- konkretizace a zobecnění (umožňuje použít obecného jevu v konkrétních podmínkách, bude využito při syntéze závěrů a implementaci),
- agregace (sloučení poznatků do uceleného přehledu, bylo využito při zpracování literárních východisek) (Disman, 2008).

Z empirických metod byla použita:

- dotazníková technika sběru dat (kvantitativní typ výzkumu),
- metoda polostrukturovaného rozhovoru (kvalitativní typ výzkumu),
- metoda přímého pozorování (kvalitativní typ výzkumu),
- případová studie (kvalitativní typ výzkumu).

Ze srovnávacích metod bude použita komparativní analýza při porovnání v rámci bankovního sektoru.

V rámci vyhodnocení kvantitativního výzkumu pomocí dotazníkové techniky sběru dat byly použity deskriptivní statistické metody (absolutní a relativní četnosti, závislosti mezi kvalitativními znaky) a faktorová analýza (vícerozměrná statistická metoda). Jednotlivé metody v rámci uvedených logických částí jsou v následujících kapitolách blíže popsány.

3. 2 Metodika disertační práce

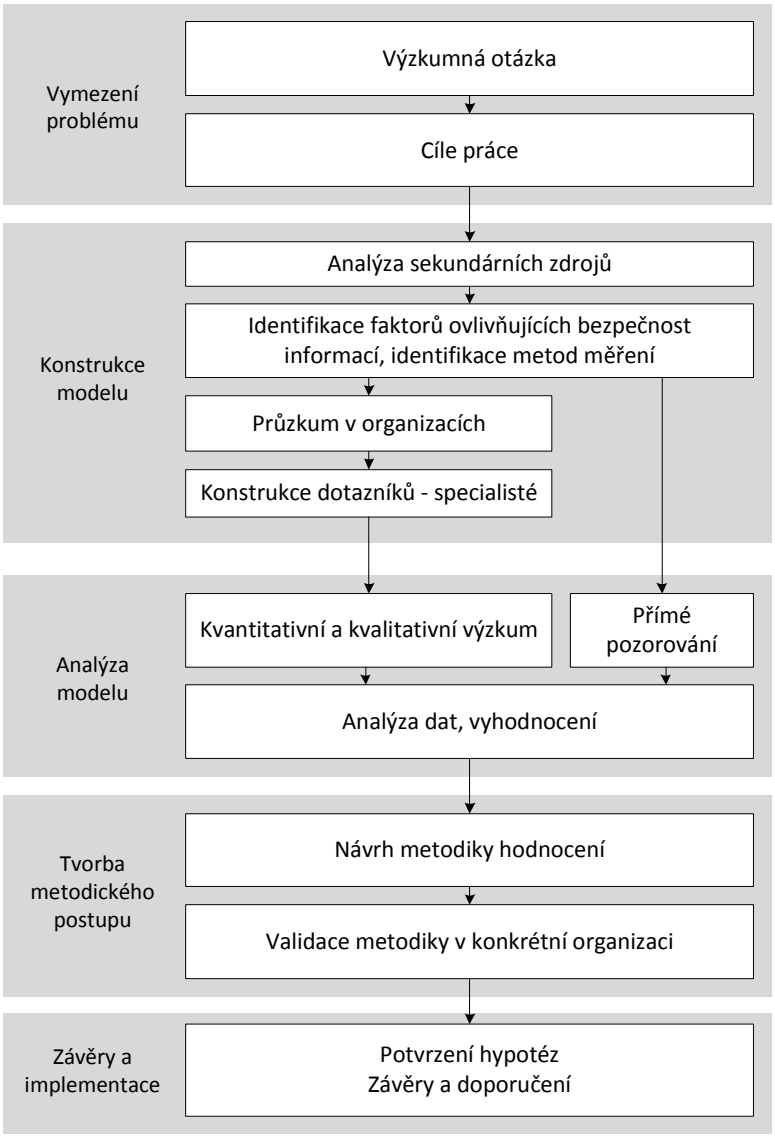
Disertační práce je rozdělena do dvou hlavních částí, které na sebe logicky navazují.

První část je tvořena literárními východisky práce (podle Disman (2008) se jedná o shromáždění aktuálních podkladů o názorech různých autorů a jejich zpracování pomocí analýzy sekundárních zdrojů a analýzy dokumentů) týkajícími se bezpečnosti informací, zahrnujícími současnou českou i zahraniční literaturu, včetně norem

a standardů. Z literárních východisek jsou na základě dedukce vyvozeny pracovní závěry, z nichž plyne stanovený hlavní cíl a dílčí cíle práce, na jejichž základě bude zpracována praktická část disertační práce.

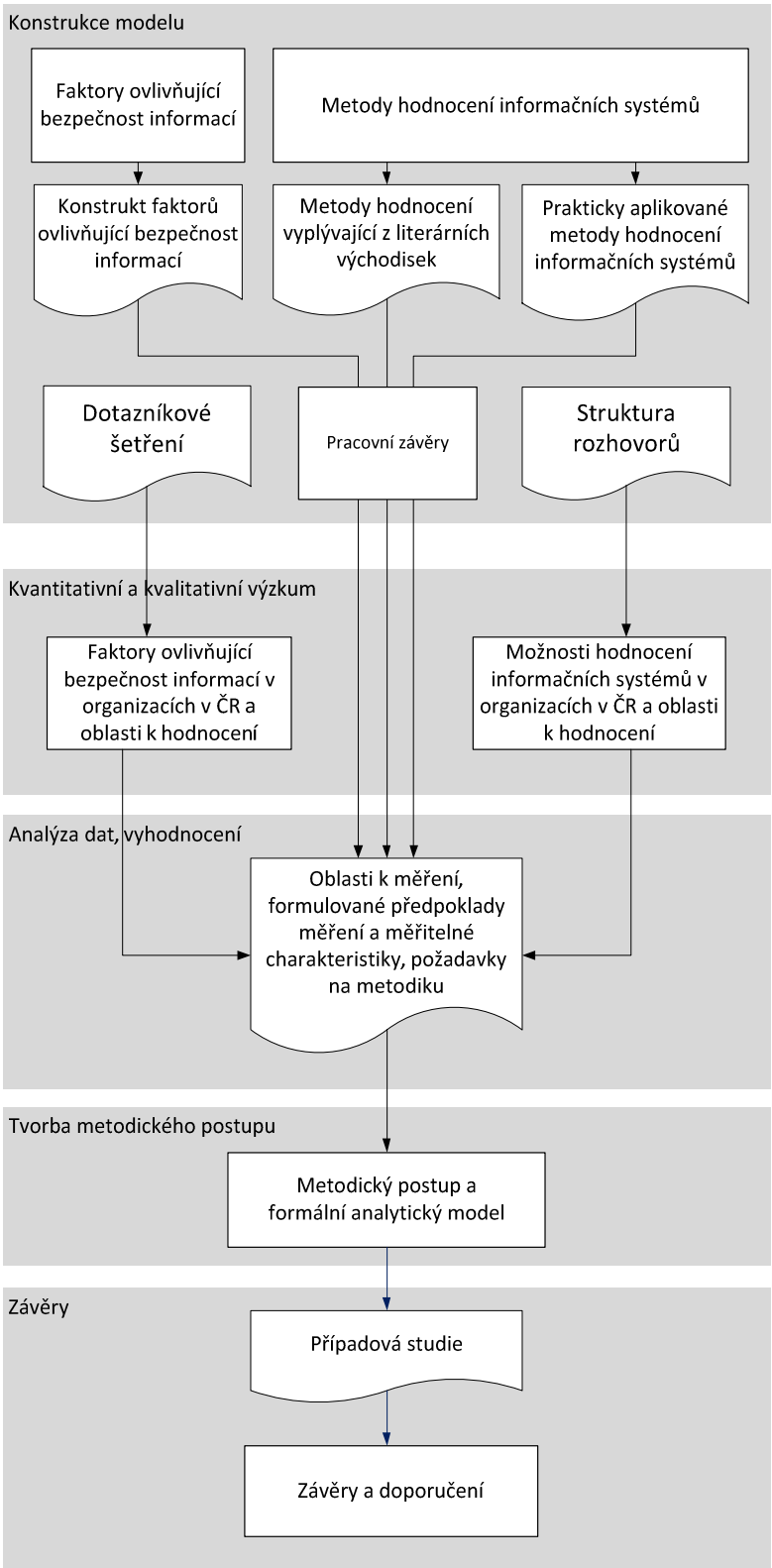
Praktická část disertační práce vychází z metodického modelu Stevenson (1989), jež je autorem upraven pro účely práce. Využívaný metodický model je tvořen čtyřmi hlavními částmi – vymezení problému, konstrukce modelu, analýza modelu a syntéza závěrů a implementace (Stevenson, 1989).

Schéma 1: Metodický postup zpracování disertační práce



Zdroj: vlastní zpracování dle Stevenson (1989)

Schéma 2: Struktura výstupů disertační práce



Zdroj: vlastní zpracování

Využití metodického aparátu v jednotlivých fázích metodického postupu (viz Schéma 1) pro vytvoření výstupů (viz Schéma 2) uvádí Tabulka 1:

Tabulka 1: Jednotlivé části metodického modelu s využitím metod výzkumu

Části metodického modelu	Teoretické metody	Empirické metody	Srovnávací metody
Vymezení problému	-	-	-
Konstrukce modelu	Analýza, agregace, dekompozice, dedukce a indukce.	Příprava dotazníkového šetření a příprava rozhovorů.	Komparativní analýza
Analýza modelu	Indukce, konkretizace, syntéza.	Dotazníkové šetření, rozhovory, přímé pozorování, faktorová a shluková analýza.	Komparativní analýza
Syntéza závěrů a implementace	Konkretizace, syntéza.	-	Komparativní analýza

Zdroj: vlastní zpracování

Lze shrnout, že v disertační práci byl proveden kvantitativní a kvalitativní výzkum zaměřený na identifikaci faktorů ovlivňujících bezpečnost informací a identifikaci měření jako prostředku hodnocení informačních systémů s cílem statisticky vyhodnotit stav hodnocení bezpečnosti informací ve vybraném odvětví. Cílem praktické části je odpovědět na stanovenou hlavní výzkumnou otázku.

Důvody, proč byl v disertační práci kombinován kvantitativní a kvalitativní výzkum, sumarizuje Tabulka 2.

Tabulka 2: Důvody využití kombinace kvantitativního a kvalitativního výzkumu

Výzkumné komponenty	Kvantitativní výzkum	Kvalitativní výzkum
Hypotézy	deduktivní	induktivní
Výzkumný soubor	náhodný, větší	záměrný, malý
Prostředí	laboratorní, modelové	přirozené, reálné
Sběr dat	objektivní nástroje	výzkumník
Projekt	determinovaný	flexibilní, možné změny
Analýza dat	statistické metody	popis, interpretace
Účast výzkumníka	většinou nepřímá	co nejvíc přímá
Vztah výzkumníka	s odstupem	těsný
Orientace výzkumníka	na vstup a výstup	na proces
Statistické zpracování	parametrické	neparametrické

Zdroj: Hendl (2006)

Cílem kombinace kvantitativního a kvalitativního výzkumu je docílení triangulace výsledků, vyjasnění kvantitativně odvozených závěrů a rovněž získání nových poznatků.

Syntézou definovaných literárních východisek, získaných výsledků výzkumu, identifikovaných rizik spojených s informacemi, identifikovaných měr pro hodnocení bezpečnosti informací v informačním systému byl formulován a popsán návrh metodiky pro hodnocení bezpečnosti informací v informačním systému organizace.

Tato metodika byla následně validována v konkrétní organizaci.

Výsledky práce (kapitola 4) jsou konfrontovány s teoretickými východisky uvedenými v literární rešerši. Ze závěrů disertační práce jsou formulovány přínosy pro další rozvoj vědního oboru a přínosy pro ekonomickou praxi.

3. 3 Kvantitativní výzkum – charakteristika

V rámci této kapitoly jsou popsány cíle kvantitativního výzkumu, návrhy použití jednotlivých metod, uvedeny předpoklady o výběrových souborech a způsobu vyhodnocení primárních dat.

Před zahájením dotazníkového šetření byl proveden průzkum, jenž testoval správnost formulování otázek a jejich pochopení respondenty, návratnost dotazníku a technickou realizovatelnost (časová náročnost, možnosti využití a třídění).

3. 3. 1 Technika sběru dat (dotazníkové šetření)

Cílem kvantitativního výzkumu bylo analyzovat úroveň hodnocení informačních systémů z pohledu bezpečnosti zpracovávaných informací, testovat stanovené hypotézy, provést analýzu kontingenčních tabulek, identifikovat rizika spojená s informacemi zpracovanými v informačním systému, identifikovat míry pro hodnocení bezpečnosti informací v informačním systému. Kvantitativní výzkum respektoval Zákon č. 101/2000 Sb. o ochraně osobních údajů a oblast etiky ve výzkumu.

Sběr dat: dotazníková technika sběru dat, byly využity výzkumné a identifikační otázky, dotazníkové šetření bylo realizováno v českém jazyce pomocí uzavřených a polouzavřených otázek. Otevřené otázky nebyly použity z důvodu nemožnosti statisticky je vyhodnotit (Řezanková, 2007).

Výběrový soubor: Organizace se sídlem v České republice využívající IT a v rámci organizace byl osloven specialista v oblasti bezpečnosti informací. Výběrový soubor organizací, které byly zahrnuty do výzkumu, byl vytvořen náhodným kvótním výběrem z organizací se sídlem v České republice prezentovaných na internetu. Organizace byly rozděleny do homogenních skupin dle výběrových kritérií odpovídajících ČSÚ tak, aby byla zajištěna reprezentativnost organizací a zobecnitelnost výsledků na výběrový vzorek. Kritéria výběru v rámci výzkumu byla stanovena tak, aby přibližně odpovídala procentnímu zastoupení organizací dle odvětví ekonomiky a velikosti organizace.

- dle odvětví ekonomiky: 15 % z primárního, 15 % ze sekundárního, 70 % z terciálního sektoru,
- dle velikosti organizace dle počtu zaměstnanců: 70 % z malých, 20 % ze středních, 10 % z velkých organizací.

Způsob zpracování dat: byl využit $\chi 2$ test pro ověření závislosti znaků v asociačních a kontingenčních tabulkách. Pokud byla vypočtená p – hodnota menší než 0,05, H_0 se na 5% hladině významnosti zamítla a byla přijata hypotéza alternativní hovořící o existenci závislosti. Síla závislosti byla zjišťována pomocí Pearsonova kontingenčního koeficientu a Cramerova kontingenčního koeficientu.

Struktura dotazníkového šetření: Struktura otázek vyplynula z definovaných hypotéz a pracovních otázek definovaných v cíli práce v kap. 2. Struktura dotazníkového šetření je uvedena v příloze, kap.10. 1.

3. 3. 2 Pilotní dotazníkové šetření

Pilotní dotazníkové šetření, v jehož rámci byla testována správnost formulování otázek, návratnost dotazníku a technická realizace, bylo realizováno v období od 10. 6. 2013 do 24. 6. 2013 a jeho výsledky byly rovněž ověřeny polostrukturovanými osobními rozhovory s respondenty, kteří jsou specialisty na oblast informační bezpečnosti. Pilotáž trvala 14 dnů a bylo osloveno 5 specialistů z vybraných organizací na sledovanou oblast. Dotazník vyplnilo všech 5 specialistů (návratnost dotazníku v pilotní fázi činila 100 %). V rámci realizovaného rozhovoru byla testována časová náročnost. Délka osobního rozhovoru byla 30-40 minut. Z pilotního šetření vyplynulo,

že otázky uvedené v dotazníku byly pro respondenty srozumitelné. Kritéria výběru v rámci předvýzkumu byla stanovena v souladu s výzkumem (viz kapitola 3. 3. 1). Soubor respondentů byl vybrán pomocí záměrného výběru a sloužil pouze pro ověření realizovatelnosti dotazníkového šetření, jeho výsledky nelze zobecnit.

Výběrový soubor pilotního dotazníkového šetření: Celkem 5 specialistů, z terciálního sektoru; 1 z malé organizace (20 %), 2 ze středních organizací (40 %), 2 z velkých organizací (40 %). V souboru oslovených manažerů bylo 5 mužů (na těchto pozicích dle statistik Ernst&Young (2011) zastává vybranou pozici 100 % mužů).

3. 3. 3 Faktorová a shluková analýza

Při vyhodnocení dat z dotazníkového šetření byla využita faktorová analýza, která patří dle Hendl (2012, s. 492) mezi vícerozměrné statistické metody, které lze charakterizovat počtem objektů n a počtem znaků (proměnných) *m*. Zdrojová matice X má rozměr *n* x *m*, kde standardně platí, že *n* je podstatně vyšší než *m*. Výpočet faktorové analýzy vychází z mezivýsledku, který tvoří korelační matice. Cílem analýzy bylo zmenšit počet proměnných (snížit dimenzi dat) a dále zjistit vztahy mezi proměnnými. Předpokladem je definice dimenze problému pomocí veličiny *m*. Faktorová analýza byla využita za předpokladu, že:

- soubor obsahoval dvě a více proměnných na „jedné straně“ (viz konstrukt faktorů ovlivňujících bezpečnost informací),
- při vyhodnocení vzájemné korelace jednotlivých závisle proměnných byly brány hodnoty pouze dostatečně vysoké (tj. větší než 0,3), to je v souladu s doporučením Anderson (2009) pro vyšší vypovídací schopnost,
- soubor statistických jednotek měl dostatečně velký rozsah. Ve výzkumu byly respektovány podmínky využití této metody dle Pacáková (2011).

Shluková analýza bude provedena za účelem rozdělení objektů do určitého systému kategorií, jež zachycuje podobnost objektů patřících do téže kategorie. Hendl (2012, s. 492) uvádí, že se hledají tzv. přirozené skupiny. Shluková analýza se zaměří na nalezení množiny shluků, přičemž jejich počet není specifikován. Další možnosti dle Hendl (2012, s. 493) zahrnují nalezení předem definovaného množství shluků, přičemž

cílem je vytvořit hierarchický strom. Shlukování bude prováděno dle Hendl (2012, s. 493) pro omezený počet objektů.

Sběr dat: dotazníková technika sběru dat viz kapitola 3. 3. 1

Výběrový soubor: viz kapitola 3. 3. 1

Způsob zpracování dat: v programu IBM SPSS Statistics, z dat získaných v dotazníkovém šetření, následně dojde ke snížení počtu sledovaných proměnných (faktorů), pomocí metody Varimax a při využití Kaiser-Guttmanovo pravidlo (tj. podstatné faktory mají hodnotu rozptylu vyšší než 1), korelační koeficienty jsou vždy v intervalu od <-1;1>. Pro vyhodnocení budou komentovány pouze hodnoty závislosti proměnných vyšší než 0,3 (středně silná závislost) dle Anderson (2009).

3. 4 Kvalitativní výzkum - charakteristika

V rámci této kapitoly jsou popsány cíle kvalitativního výzkumu, návrhy použití jednotlivých metod, uvedeny předpoklady o výběrových souborech a způsobu vyhodnocení primárních dat.

3. 4. 1 Polostrukturované rozhovory

Cílem kvalitativního výzkumu bylo vytvoření nových hypotéz, nové teorie na základě zodpovězení výzkumných otázek. Výzkum byl anonymní.

Sběr dat: polostrukturovaný rozhovor, průměrná doba trvání 30 – 45 minut, nahrávání na diktafon.

Výběrový soubor: záměrný výběrový soubor, specialisté v oblasti bezpečnosti informací v bankovních institucích.

Způsob zpracování dat: naplnění saturace u výzkumných otázek.

Struktura rozhovorů: podle seznamu otázek v kap.10. 2, které byly rozděleny do skupin Práce s informacemi, zralost procesů informační bezpečnosti a hodnocení.

3. 4. 2 Přímé pozorování

Cílem této metody bylo podpořit výsledky předchozích metod. Jedná se o výzkumnou metodu, při níž se sleduje a zaznamenává nebo popisuje činnost lidí, předmětů, se kterými manipulují, prostředí aj. Jde o subjektivní metodu (Disman, 2008).

Sběr dat: přímé zúčastněné pozorování.

Výběrový soubor: Specialisté v oblasti bezpečnosti informací v bankovních institucích a společnostech – Česká spořitelna a.s., Komerční banka a.s., ČSOB a.s, CGI IT Czech Republic s.r.o.

Způsob zpracování dat: případová studie zahrnující doporučení a návrhy pro hodnocení informačních systémů z pohledu bezpečnosti zpracovávaných informací.

3. 4. 3 Komparativní metoda

Cílem bylo provedení komparace vlivu jednotlivých faktorů ovlivňující hodnocení informačních systémů z pohledu bezpečnosti zpracovaných informací v bankovním sektoru a jiných odvětvích ekonomiky dle CZ-NACE.

Stanovená kritéria: Rozdíly faktorů hodnocení dle velikosti organizace, faktory ovlivňující hodnocení informačních systémů v primárním, sekundárním a primárním sektoru a dále specifika v bankovním sektoru.

Sběr dat: v rámci kvantitativního a kvalitativního výzkumu.

Výběrový soubor: stanovení v rámci kvantitativního a kvalitativního výzkumu (kapitola 3. 3 a 3. 4).

3. 5 Tvorba metodického postupu – charakteristika

Cílem bylo vytvoření metodického postupu pro hodnocení bezpečnosti informací v informačním systému na bázi standardu ISO/IEC 27004:2009.

Stanovená kritéria: aplikovatelnost měr v procesu měření dle ISO/IEC 27004, přínosy v oblasti řízení rizik pro informace v informačních systémech organizace a v procesu auditu pro stanovení slábnoucí oblasti.

Postup tvorby: na základě syntézy výstupů analýzy sekundárních zdrojů a výstupů analýzy dat získaných v rámci provedených výzkumů byl formulován metodický postup. Metodický postup je ověřen na reálné organizaci. K výpočtům v rámci analytického modelu byl použit nástroj MATLAB verze 2015R a Microsoft Excel 2010.

3. 6 Případová studie - charakteristika

Cílem byl návrh metodiky hodnocení bezpečnosti informací v informačním systému pro vybranou organizaci v bankovním sektoru v rámci ČR, kde následně proběhla validace navržené metodiky.

Ve výzkumu a při verifikaci výsledků byly zkoumané organizace na základě požadavků zástupců organizace, ve kterých probíhal výzkum, anonymizovány. V rámci první případové studie je název banky změněn na A a v rámci IT společnosti s většinovým zahraničním podílem je využita zkratka B.

Sběr dat: v kvantitativním a kvalitativním výzkumu a přímým pozorováním.

Typ případové studie: instrumentální (Hendl, 2012, s. 105).

Výběrový soubor: záměrný výběr, návrh metodiky pro organizaci A, B.

Způsob zpracování dat: vyhodnocení výzkumu, návrh metodiky, ověření v praxi, formulace doporučení, závěrů z toho plynoucí. K výpočtům a prezentaci výsledků byl použit nástroj MATLAB verze 2015R a Microsoft Excel 2010.

Procedura zpracování případové studie:

- Na vybrané organizaci v **ekonomickém odvětví** „finanční služby“ byla zvolena **oblast** jako cíl hodnocení. Hranice oblasti je zvolena tak, aby byla uzavřená z pohledu použitých informačních a komunikačních technologií, tj. např. samostatnou **organizační jednotkou.** Oblastí je *Přímé bankovnictví*. Okolí oblasti je považováno za ideální z pohledu zkoumané problematiky.
- Na vybrané organizaci v **terciálním sektoru** byla zvolena **oblast** jako cíl hodnocení bezpečnosti informací. Hranice oblasti je zvolena tak, aby byla uzavřená z pohledu použitých informačních a komunikačních technologií, tj. např. samostatnou **organizační jednotkou.**
- V rámci oblasti byly identifikovány informační systémy, byly dekomponovány a byl aplikován **metodický postup** hodnocení a identifikovány míry do **formálního analytického modelu**. Identifikace systémů, míry a hodnoty parametrů vyplynuly z výzkumu a přímého pozorování.
- Metodický postup a výstupy formálního analytického modelu byly validovány proti očekávaným hodnotám na základě informací z vybrané oblasti.

4 REŠERŠE SOUČASNÉHO STAVU

V rámci kapitoly (rešerše současného stavu) je vytvořen aktuální přehled problematiky a tvoří základ pro praktickou část práce. Kapitola obsahuje definice podstatných pojmů, pokrytí tématu v dostupných zdrojích a vyvození východisek pro praktickou část práce.

4. 1 Definice pojmů

Definice pojmů v různých zdrojích jsou u některých pojmů rozdílné. Při výběru termínů se primárně vychází z definicí uvedených v ČSN, resp. definicí uvedených v mezinárodních normách ISO. V částech, které nejsou upraveny normami, se vychází z mezinárodních pramenů.

Data jsou opakovaně interpretovatelná formalizovaná podoba informace vhodná pro komunikaci, vyhodnocování nebo zpracování (ČSN ISO/IEC 2382-1, 1998, s. 8). Na data lze pohlížet jako na od přírody objektivní reprezentanty lidí, objektů, událostí a pojmů (Požár, 2005, s. 22). Pojem data je chápán jako profesionální označení pro čísla, text, zvuk, obraz, případně další smyslové vjemy. Data vznikají čtením, pozorováním, měřením, výpočtem, vážením apod. (Požár, 2005, s. 25). Z této definice lze vyvodit, že za data lze považovat i jiné fyzikální veličiny, které lze zprostředkovaně vnímat či transformovat do výše uvedených. Data se přenáší, zpracovávají a předávají (Požár, 2005, s. 25). Podle dalších historických definicí např. v Krištoufek (1982, s. 34) jsou za data považovány jakékoliv údaje zpracovávané programem. Z definicí je zřejmé, že data jsou obvykle zpracovávána technickými, resp. programovými prostředky procesem zpracování dat, kterým mohou být transformována a organizována do uživatelem vnímatelné formy.

Zpracování dat je systematické provádění operací s daty např. aritmetické nebo logické operace s daty nebo třídění dat, sestavování nebo kompilace programů a dále operace s textem např. úprava, třídění, slučování, ukládání, vyhledávání, zobrazování nebo tisk (ČSN ISO/IEC 2382-1, 1998, s. 8). Smyslem zpracování dat je vytvoření informace (Požár, 2005, s. 22). Zpracování dat se provádí u dobře strukturovaných úloh

za použití klasických metod, jakými jsou statistické metody, metody operační analýzy, metody hromadné obsluhy apod. U špatně strukturovaných úloh se používají metody jako fuzzy logika, expertní systémy, umělé neuronové sítě, genetické algoritmy, tedy převážně metody na bázi umělé inteligence (Smejkal, Rais, 2006, s. 174).

Systém zpracování dat je jeden nebo více počítačů, periferních zařízení a programů použitých pro zpracování dat (ČSN ISO/IEC 2382-1, 1998, s. 8).

Informace je podle ČSN ISO/IEC 2382-1 (1998, s. 7) poznatek týkající se jakýchkoliv objektů, například fakt, událostí, věcí, procesů nebo myšlenek, včetně pojmů, který má v daném kontextu specifický význam. Informací může být jakýkoliv energetický či hmotný projev, který může mít smysl buď pro toho, kdo sděluje nebo pro toho, kdo sdělované přijímá (Mates, Matoušová, 1997, s. 27). Podle Mládkové (2004) jsou informace definovány jako data, kterým jejich uživatel při interpretaci přiřazuje důležitost, neboli význam dat, jak je chápe člověk. Informace vzniká z dat v okamžiku přiřazení do kontextu a nesou význam pochopitelný lidmi (Slovník výpočetní techniky in Smejkal, Rais, 2006, s. 171). Informace je z definice subjektivní a existuje jenom ve vztahu k příjemci-uživateli. Informace o nějakém jevu, procesu, události je jistá veličina, která snižuje dosavadní neurčitost právě o tomto jevu, události (Požár, 2005, s. 22). Pojem informace je obecně vymezován z pohledu:

- matematické teorie informace, tj. matematické reprezentace podmínek a parametrů ovlivňující přenos a zpracování informací (Shannon);
- kybernetiky, tj. systémů řízení procesů v živých organismech a strojích (N. Wiener);
- obecné teorie systémů, tj. abstraktní organizace prvků bez ohledu na jejich substanci, typ nebo prostorové či časové podmínky jejich existence (K. L. von Bertallanfy);
- počítačové vědy, informatiky, tj. architektury a programy počítačů a oblastí jejich využití včetně technologie zpracování a přenosu informací (J. von Neumann);
- sociální komunikace, tj. sdělování a vyměňování informací ve společnosti;
- informační vědy (sociální informatiky), tj. funkcí a struktur informací a procesů získávání, zpracování, přenosu a využívání informací ve společnosti.

Informace jsou obecně chápány:

- jako ekonomický zdroj,
- jako výrobní faktor,
- jako komodita (zboží), kdy informace jsou produktem či službou,
- jako konkurenční výhoda,
- jako prostředek řízení organizace – nezbytné pro správné rozhodování a snížení informačního rizika (stupně složitosti) při rozhodování (nedostatek či přebytek) (Drucker, 1998, s. 35; Smejkal, Rais, 2006, s. 170),
- jako hnací prostředek megatrendů managementu,
- jako základna pro tvorbu znalostí (Drucker, 1998, s. 35),
- prostředek informační války a terorismu (Požár, 2005, s. 11).

Informace je jednoznačně považována za aktivum s vlastní proměnnou hodnotou (Drucker, 1998, s. 35; Dobda, 1995, s. 12).

Dle Požár (2005, s. 25) ve vztahu mezi daty a informacemi platí, že každá informace je reprezentována daty (datem), ale data (datum) nemusí vždy konstituovat informaci. Z pohledu tohoto vztahu je vždy tedy nutno uvažovat tři stavy, tj. že data reprezentují informaci, přestože nemusí být při zpracování dat zřejmá, že data informaci nereprezentují (jedná se o šum), a že data informaci nereprezentují v danou chvíli, ale po doplnění dalších dat mohou přejít do jednoho z dříve uvedených stavů nebo zůstat v tomto stavu.

Zpracování informací podle ČSN ISO/IEC 2382-1 (1998, s. 8) je systematické provádění operací s informacemi zahrnující zpracování dat a případně i datovou komunikaci a automatizaci kancelářských prací. Podle Drucker (1998, s. 5) probíhá tvorba informací na základě zpracování dat, přičemž jsou využívány znalosti. Zpracování informací je tedy proces, který je schopen provádět pouze subjekt, který je schopen aplikovat znalosti.

Automatizace kancelářských prací je forma integrace kancelářských prací pomocí systému zpracování dat (ČSN ISO/IEC 2382-1, 1998, s. 8). S ohledem na penetraci informačních technologií a moderní způsoby komunikace jsou kancelářské práce chápány jako podstatně širší pojem, zahrnují nejen práci v kanceláři a práci

managementu v organizacích, ale také práci koncových uživatelů, technologických pracovníků, vědců apod., které probíhají v domácím prostředí, v továrnách a vědeckých pracovištích apod.

Informační proces je dle Požár (2005, s. 29) provádění pracovních činností s informacemi za účelem změny procesů, činností a chování organizace. Informační proces je uzavřený cyklus, kterým informace prochází od svého vzniku až ke svému užití. Obecný informační proces odkazovaný v literatuře (Doucek et al., 2011, s. 37; Požár, 2005, s. 29) zahrnuje sled operací s daty a informacemi, který obsahuje kroky:

- Získávání (sběr) informací – informace získává uživatel měřením, pozorováním, čtením, odposlechem, studiem (Požár, 2005, s. 29), obecně lze však informace získat dalšími způsoby, tj. nákupem, výpůjčkou, vytvořením kopie (stažením), záznamem. Jde o časově a systémově uspořádané pořizování dat, jimž následně přiřazuje uživatel význam. Získané informace jsou obvykle odborné, právní, ekonomické, o okolním prostředí organizace, zahraniční, všeobecné, organizačně technické, personální, o vlastním informačním systému, specifické apod. (Požár, 2005, s. 29).
- Registrace (evidence) a ukládání informací – zajišťuje vytváření spisového či administrativního pořádku. (Požár, 2005, s. 33). Registrace zahrnuje kroky katalogizace, indexování, klasifikace (třídění), agregace, konverze, lokalizace. Podstatná je kvalita uložení, na systému uchovávání závisí rychlost a kvalita pozdějšího využívání (Požár, 2005, s. 33). Kvalitu uložení lze považovat za podstatnou primárně pro informační systémy založené na papírových procesech, platí však obecně i pro počítačové informační systémy, kdy rozsáhlé množství dat za použití výpočetní techniky může kvalitou uložení ovlivnit schopnost informace zpracovávat včas.
- Přenos informací – předávání informací mezi prvky uvnitř informačního systému a mezi informačními systémy (obvykle fyzicky oddělenými). Přenos probíhá na bázi transformace informace do datové podoby a následném kódování na straně odesílatele, samotném přenosu prostřednictvím přenosového kanálu a dekódování a následném převodu do datové podoby na

straně příjemce, kde je transformována zpět do informace. Cílem je omezit při přenosu rušivé vlivy a zkreslení informace (Požár, 2005, s. 31).

- Zpracování informací – účelové, za určitým cílem prováděné zpracování informací (Požár, 2005, s. 34). Cílem je obvykle následné provedení analýzy a syntézy. Zahrnuje podprocesy (třídění, filtrování a slučování dat, vymezení informačních významů), které jsou uskutečňovány účelově s cílem vytvořit obraz požadované skutečnosti.
- Využívání informací - vlastní cíl informačního procesu. Informace mohou být využity přímo jejich zpracovatelem, případně přeneseny (Požár, 2005, s. 34). To upřesňují další zdroje, které za využívání považují **distribuci informací**, tj. výdej zpracovaných dat uživatelům a **prezentaci**, tj. zobrazení dat příjemcům ve srozumitelné formě. Účel prezentace určuje formu zobrazení, např. textovou zprávu, grafické zobrazení, případně multimediální prezentaci integrující vizuální a zvukovou prezentaci.
- Likvidace informací – součást životního cyklu informace je jejich likvidace (Dobda, 1998, s. 11).

Informace se v informačním procesu využívají k ovlivňování technologických, manažerských, informačních a dalších procesů. Týkají se především vztahů lidí k manažerské aktivitě, vztahů mezi sebou, jejich vzájemného působení, potřeb, zájmů, cílů apod. (Požár, 2005, s. 24).

Informační systém je dle ČSN/ISO IEC 2382-1 (1998, s. 9) definován jako systém zpracování informací spolu s návaznými organizačními prostředky, např. personálem, technickými a funkčními prostředky. Informační systém:

- je systém, který je formálně definován jako množina $S = (A, R)$, kde A je neprázdná množina prvků a R je množina všech závislostí (Klír in Požár, 2005, s. 27), resp. jako konečná množina prvků (Q) a množina vazeb mezi nimi (a) s dynamickým a účelovým chováním $S = (Q, a)$(Vlček in Požár, 2005, s. 27). Systém má hranici a okolí. Systém je abstrakcí reálného objektu, kterou je možno definovat určitými prvky (Požár, 2005, s. 27).

- je soubor lidí (zdrojů, zpracovatelů, uživatelů), technických prostředků a metod zabezpečujících sběr, přenos, uchování a zpracování dat za účelem tvorby a prezentace informací pro potřeby uživatelů (Požár, 2005, s. 26).
- zahrnuje všechny informační procedury (formální i neformální), které v organizaci probíhají (Smejkal, Rais, 2006, s. 41).

Lze shrnout, že informační systém je soubor prvků s účelově uspořádanými vazbami a účelovou funkčností (strukturou vč. hierarchických vztahů, pravidel a norem) a informačními a datovými toky mezi těmito prvky, kde primárním účelem toků je přenos informací. Cílem informačního systému je umožnit realizaci informačního procesu za účelem podpory podnikových obchodních cílů. Prvky informačního systému, které se účastní informačního procesu, jsou:

- informace, jako hlavní předmět činnosti informačního systému (v elektronické, písemné resp. audiovizuální a ústně předávané podobě) (Požár, 2005, s. 57, s. 87),
- uživatelé, lidé, osoby – sdělovatelé (poskytovatelé) informací, příjemci informací (klienti) (Požár, 2005, s. 87), zpracovatelé spouštějící zpracování informací, správci, zprostředkovatelé informací; za uživatele lze za určitých okolností považovat obecný subjekt, pokud je schopen pracovat v uvedených rolích,
- systémy zpracování dat a informací (informační infrastruktura) a všechny jejich hmotné i nehmotné součásti – hardware (počítače a periferie, síťové prvky), software (aplikace, programy, jazyky), pracovní postupy, techniky a metody, materiál a nemovitosti (Požár, 2005, s. 87).

Historicky byly informační systémy:

- klasické manuální neautomatizované – zahrnují prostředky a procesy, tedy písemné dokumenty, rukou psané poznámky, telefonické hovory, obchodní jednání, jednání představenstva, poštovní zásilky, vnitropodniková pošta,
- počítačově orientované – automatizované informační systémy postavené na informačních a komunikačních technologiích.

Míra (angl. measure) dle ISO/IEC 15939 (2007, s. 2) je definována jako proměnná, které je přiřazena hodnota měřeného atributu jako výsledek procesu měření, přičemž atribut je vlastnost nebo charakteristika entity, která může být zjištěna kvantitativně nebo kvalitativně automatizovanými prostředky nebo člověkem. Autor v dalším textu jednotně používá termín „míra“ v souladu s anglickými verzemi normativů, tedy nepoužívá termín „metrika“ z českého překladu ISO 27004.

Metrika[2] (angl. metric) je v literatuře využívána v různých kontextech:

- nástroj pro usnadnění rozhodování a zlepšování výkonnosti a zodpovědnosti sběrem, analýzou a reportováním relevantních výkonnostně orientovaných dat (Chew at al., 2008, s. 9). Umožňuje nápravné akce na základě změřených hodnot.
- Na vyšší úrovni je metrika kvantifikovatelné měření konkrétního aspektu systému nebo podniku. Pro entitu (systém, produkt nebo jiný) existují identifikovatelné atributy a metrika vyjadřuje, jak mnoho z tohoto atributu entita vlastní. (SSE-CMM: Systems Security Engineering capability maturity model in Jansen (2009, s. 3)).
- Podle Savola (2007, s. 28) a Jansen (2009, s. 3) metrika obecně znamená proces a metodu kvantifikace daného atributu, aspektu nebo charakteristiky. Savola (2010, s. 230) uvádí, že metrika “*[...] zjednodušuje komplexní socio-technický systém do modelů a dále do čísel, procent nebo částečného pořadí*“.
- Kvantifikovaná entita, která umožňuje hodnocení míry dosažení cíle procesu v porovnání s předchozím stavem. Vyjadřuje výkon (ang. performance). Metrika by měla být SMART (specifická, měřitelná, akceschopná, relevantní, časově ukotvená).

[2] Pojem „metrika“ má několik významů a používání pojmu „míra“ v zahraničí ani v české republice není zcela harmonizováno. Nesoulad vychází z nejednoznačného překladu a používání v odborné literatuře v porovnání s normativy. Např. v českém překladu normy ISO 27004:2009 je jako překlad pojmu „measure“ použita „metrika“. Americká literatura také používá výhradně „metric“ a anglické normativy pak „measure“. Konkrétní význam je pak třeba posuzovat podle kontextu.

- Pojem z teorie metrických prostorů, jehož spojení s oblastí informačních technologií je nevhodný (Jansen, 2009, s. 4).

Postup uplatnění metrik zahrnuje následující aktivity:

- Identifikace problémových oblastí a jejich priorit – na základě informací o stavu skutečností jsou stanoveny problémy a rizika a jejich priorita.
- Výběr kategorie metrik a stanovení metrik – kategorizace metrik s analogickým zaměřením. Metriky jsou dále stanoveny (mapovány) na základě kategorie (finanční kategorie využívá finanční metriky, využití zdrojů zahrnuje měření využití parametrů konkrétních zdrojů apod.).
- Sběr dat – provádění měření.
- Normalizace dat pro měření – stanovení převodních pravidel a modelů pro porovnání dat s rozdílnými charakteristikami s cílem aplikovat shodná agregační a normalizační pravidla na data z různých primárních zdrojů (Učeň, 2001, s. 89).
- Analýza naměřených dat – výsledky měření a kvalitativní hodnocení společně mohou vést ke korekci či identifikaci nových problémových oblastí (Učeň, 2001, s. 89).
- Rozhodování na základě analyzovaných dat – zahrnuje periodické hodnocení, doplňující otázky a další činnosti vyplývající z analyzovaných naměřených dat.

Metrika je definována:

- identifikačním názvem,
- algoritmem, resp. vzorcem u tvrdých metrik resp. definicí u měkkých metrik,
- dimenzí (měrná jednotka, organizační jednotka, časové období),
- výchozí a cílovou hodnotou,
- zdrojem dat pro měření,
- metodikou měření,
- metodikou ověřování výsledků (Učeň, 2001, s. 34).

Typy metrik podle (Učeň, 2001, s. 34) jsou:

- tvrdé metriky – objektivně měřitelné ukazatele, které v ideálním případě přímo ovlivňují základní konkurenční faktory. Ukazateli jsou taktéž indikátory, u nichž jsou stanoveny žádoucí meze nebo horní či dolní limit,
- měkké metriky – hodnotící prostředek sloužící k měření a hodnocení jednotlivých procesů či funkčních oblastí auditním způsobem (Učeň, 2001, s. 34).

Existence metrik a schopnost kvantifikovat veličiny v problémové oblasti jsou indikátorem dobře strukturované úlohy (Smejkal, Rais, 2006, s. 173).

Riziko je pravděpodobnost, že dojde k nepříznivému odchýlení skutečného stavu od očekávaného, přičemž vzniká určitá ztráta. Kategorie rizika vyplývá z konkrétní podmínky reálného světa. Riziko je obvykle oborově specifické, tedy např. ekonomické, politické, bezpečnostní, právní, manažerské, specifické apod. (Smejkal, Rais, 2006, s. 79).

Bezpečnost v širším smyslu (angl. safety) je kvalita nebo stav, kdy jsou zdraví, resp. zájmy objektu ochráněny (angl. safe) před vlivem nebo způsobením fyzického poškození, zranění nebo ztráty (Merriam-Webster, 2013). Tyto faktory jsou chápány ve smyslu nežádoucích fyzických, sociálních, duchovních, finančních, politických, emočních, psychologických důsledků selhání, poškození, chyby, nehody či ohrožení. Za bezpečný je považován ustálený stav, ve kterém objekt vykazuje očekávané chování.

Bezpečnost v užším smyslu (angl. security) vyjadřuje stav, kdy objektu nehrozí nebezpečí, nebo není vystaven riziku ztráty (Merriam-Webster, 2013). Vyjadřuje stupeň ochrany objektu proti nebezpečí, poškození, ztráty vyplývající ze záměrné aktivity. Záměrná aktivita narušuje ustálený stav objektu, ve kterém vykazuje očekávané chování.

Souhrnně se bezpečností rozumí stav, kdy jsou na akceptovatelnou míru eliminovány hrozby pro objekt a jeho zájmy. Objektem může být stát, organizace, systém, sociální skupina (národ, národnostní menšina, jednotlivec) (Smejkal, Rais, 2006, s. 41). Bezpečnost je vlastnost objektu, která určuje stupeň, míru ochrany proti

možným škodám a hrozbám (Požár, 2005, s. 37). Dosažení konkrétní akceptovatelné míry bezpečnosti konkrétního objektu je tedy cílový stav, jehož je dosahováno systematickými prostředky a procesy ochrany. Systematické zajišťování ochrany slouží k poznání a eliminaci vnějších a vnitřních bezpečnostních rizik.

Bezpečnostní perimetr je pomyslná hranice bezpečnostní omezené oblasti, ve které jsou v činnosti a platnosti objekty, které vynucují a udržují požadovanou bezpečnostní úroveň a kontrolní opatření za účelem ochrany hodnot (Dobda, 1998, s. 79). Perimetr tedy vymezuje rozhraní mezi vnější (nechráněnou) a vnitřní (chráněnou) oblastí bezpečnosti. Perimetr vychází z principů zónové ochrany (ochrana konkrétního objektu nebo oblasti).

Ochrana objektu představuje činnosti pro dosažení a udržení bezpečnosti tohoto objektu. Primárně jsou chráněným objektem vybraná aktiva s hodnotou (Dobda, 1998, s. 14). Ochrana je aplikována v rámci bezpečnostního perimetru s tím, že její dosah a vliv může být za hranicí tohoto perimetru.

4. 2 Kvalitativní charakteristiky informace a informační proces

Každá informace disponuje vlastnostmi, které mají vliv na její vlastní kvalitu. Kvalita informace je z její definice závislá na kvalitě dat a kvalitě transformačního procesu informace.

ISO/IEC 25012 in Natale (2015, s. 2) kategorizuje kvalitativní charakteristiky dat podle dvou perspektiv – inherentní a systémově závislé, přičemž všechny charakteristiky mají stejnou důležitost (Natale, 2015, s. 2). Podle ISO/IEC25012 in Natale (2015, s. 2):

- *inherentními (vnitřními) charakteristikami* jsou přesnost (angl. accuracy), úplnost (angl. completeness), konzistentnost (angl. consistency), věrohodnost (angl. credibility), aktuálnost (angl. currency);
- *inherentními a systémově závislými* jsou přístupnost tělesně postiženými (angl. accessibility), soulad se standardy (angl. compliance), důvěrnost (angl. confidentiality), efektivnost (angl. efficiency), přesnost (angl. precission), sledovatelnost (angl. traceability), srozumitelnost (angl. understandability);
- *systémově závislými* jsou dostupnost (angl. availability), přenositelnost (angl. portability), obnovitelnost (angl. recoverability).

ISACA (2013, s. 31) definuje pro kvalitu informace tato kritéria:

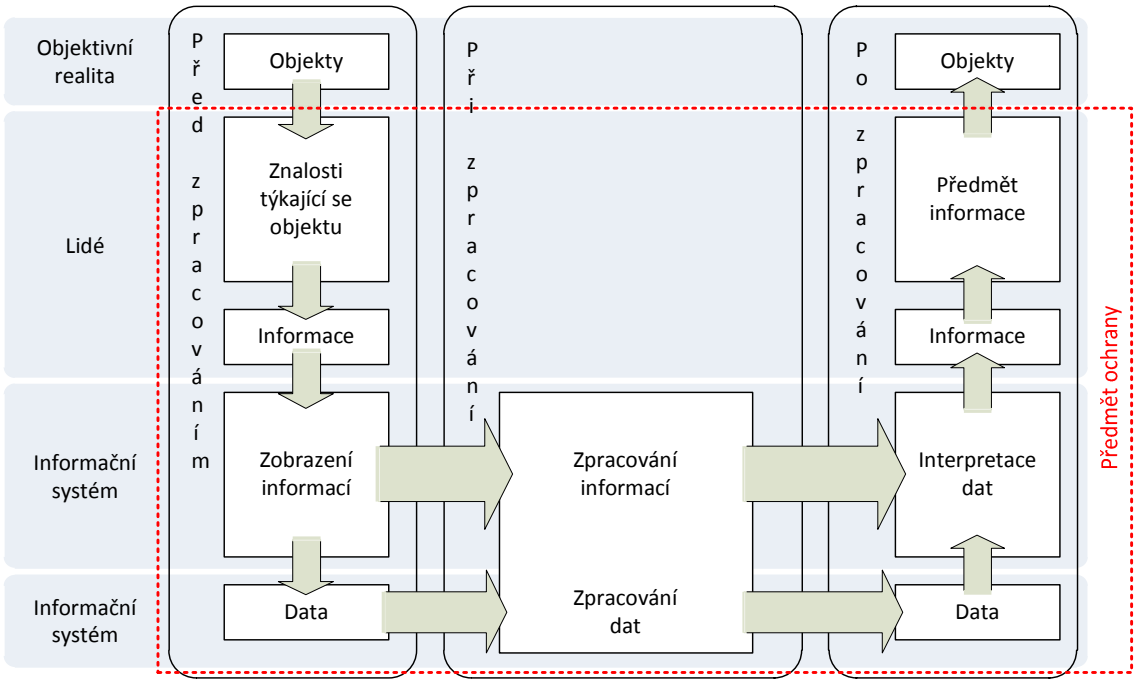
- *intrinsické (vlastní),* které zahrnují přesnost (angl. accuracy), objektivnost (angl. objectivity), věrohodnost (angl. beliveability), reputace (angl. reputation);
- *kontextuální,* které zahrnují relevantnost (angl. relevancy), kompletnost (angl. completeness), aktuálnost (angl. currency), přiměřenost (angl. appropriate amount), stručná reprezentace (angl. concise representation), interpretovatelnost (angl. interpretability), srozumitelnost (angl. understandability), snadnost manipulace (angl. ease of manipulation);
- *bezpečnostní,* které zahrnují dostupnost (angl. availability) a omezený přístup (angl. restricted access).

Další zdroje doplňují a upřesňují kvalitativní charakteristiky informace:

- Relevantnost – charakter informace by měl odpovídat charakteru jejího užití.
- Správnost – informace by měla být pravdivá a spolehlivá. Měla by mít přijatelnou přesnost. Informace musí vytvářet reálný obraz světa (Peltier, 2002, s. 108).
- Včasnost – informace je třeba předávat v pravý čas, tj. v době jejich potřeby a užití. Informace by měly být dostupné a kompletním ve správnou chvíli v komplexním množství (pro snížení míry tzv. halo efektu prvotního postoje) (Smejkal, Rais, 2006, s. 170).
- Ověřitelnost – informace je jednoznačně svázána se zdrojem, ze kterého byla získána.
- Věrohodnost – informace by měla pocházet z ohodnoceného zdroje. Existují různé klasifikace informací z pohledu věrohodnosti, např. kodifikace 4x4 dle Brabec a kol. in Smejkal, Rais (2006, s. 191).
- Aktuálnost – informace by měly co nejlépe odrážet aktuální skutečnost. Informace má časovou platnost (Smejkal, Rais, 2006, s. 190).
- Úplnost – je třeba, aby byly k dispozici veškeré požadované informace. Nedostatečné poznání skutečnosti v důsledku neúplných informací zavádí do rozhodování rizika (Smejkal, Rais, 2006, s. 172). Podstatná je tedy maximalizace úplnosti informací.
- Přiměřenost – informace by měly být přiměřeně podrobné. Existuje optimum množství relevantních informací v určitém čase. Nedostatek informací je překážkou rozhodování (zdroj rizik), velké množství informací, které nelze bezprostředně využít taktéž (Smejkal, Rais, 2006, s. 170).
- Nákladová přiměřenost zpracování informace – vyžaduje-li získání nebo zpracování potřebné informace nepřiměřeně dlouhou dobu nebo nadměrné úsilí vzhledem k užitku, který poskytuje, nelze ji považovat za nákladově přiměřenou.

Základní transformační proces informace je popsán schématem zpracování informací podle v ČSN/ISO IEC 2382-1 (1998, s. 9). Schéma je doplněno o horizontály označující subjekty, v nichž daná fáze probíhá a oblast působení ochrany informací.

Schéma 3: Základní transformační proces informace



Zdroj: ČSN/ISO IEC 2382-1 (1998, s. 9), upraveno a doplněno autorem

V jednotlivých fázích transformačního procesu se informace nacházejí v jednom ze základních stavů jejich životního cyklu: v užívání (angl. „in use“), v přenosu (angl. „in motion“) a v uloženém stavu (angl. „at rest“). Mezi těmito stavy informace přecházejí. To potvrzuje CNSS (Committee on National Security Systems) in Whitman (2010, s. 5). Je zřejmé, že informace jsou v informačním procesu v užívání při krocích zpracování a využívání informací, v přenosu při získávání informací, registraci, ukládání, a informace mohou být uloženy v prostředcích počítačové techniky, v psané formě či v lidské paměti (Smejkal, Rais, 2006, s. 147).

Je zřejmé, že kvalita informací, které procházejí transformačním procesem, přímo ovlivňuje jeho výstupy, tedy schopnost objektivního poznání skutečnosti a poznání předmětu informace. Je taktéž zřejmé, že **hodnota informace** je přímo úměrná kvalitě informace, kvalitě dat a transformačního procesu. Jakékoliv vlivy působící na kvalitu

informací přímo nebo nepřímo ovlivněním transformačního procesu pro uživatele znamenají ztrátu části nebo celé hodnoty informace. Naopak opatření, která působí proti těmto vlivům, pomáhají kvalitativní charakteristiky zachovat a ochránit. Předmět aplikace opatření tvoří součásti transformačního procesu - **informační systém** a **lidé**.

4. 3 Rizika a nejistota

Ke stavům světa se váží prvky rozhodovacího procesu - jistota, riziko a nejistota. Tyto prvky ovlivňují typ rozhodovacího procesu. Veber a kol. (2000) rozlišují rozhodovací procesy za jistoty, rizika a nejistoty. Toto členění rozhodovacích procesů vychází z míry informací o budoucích hodnotách faktorů ovlivňujících důsledky variant rozhodování (tzv. stavy světa, resp. scénáře), a tím tedy i z míry informací o těchto důsledcích.

V případě úplné informace, tzn., že rozhodovatel ví s jistotou, který stav světa nastane a jaké budou důsledky variant, se jedná o rozhodování za jistoty. Pokud rozhodovatel zná možné budoucí situace (stavy světa), které mohou nastat a tím i důsledky variant při těchto stavech světa a současně zná i pravděpodobnosti jednotlivých stavů světa, pak jde o rozhodovací proces za rizika. Pokud nejsou rozhodovateli známy pravděpodobnosti stavů světa, jde o rozhodování za nejistoty. Terminologie však není jednotná a někteří autoři používají k označení rozhodování za nejistoty termín rozhodování za neurčitosti (Veber a kol., 2000).

Riziko je z hlediska problematiky řízení podnikatelských rizik chápáno jako možnost, že s určitou pravděpodobností dojde k události, jež se liší od předpokládaného stavu či vývoje (Pearce in Smejkal, Rais, 2006, s. 78). O riziku lze hovořit pouze v případě, kdy výsledek je nejistý, tedy existují alespoň 2 varianty řešení. Současně musí platit, že jedna z variant řešení je nežádoucí. Toto potvrzuje Holand in Merna (2007, s. 9), když tvrdí, že riziko je nechtěným důsledkem jevu, který je nejistý s chtěnými i nechtěnými důsledky.

Při rozhodování za rizika jsou známy pravděpodobnosti realizace jednotlivých stavů okolností, tj. je znám vektor rizika

$$p = (p_1, p_2, \ldots p_n)^T$$

přičemž platí:

$$\sum_{j=1}^{n} p_j = 1 \text{ a pro všechna } j \text{ platí } p_j \geq 0 .$$

Nejistota existuje tam, kde existuje více než jeden možný výsledek, ale pravděpodobnost konkrétního výsledku není známa (Kouns, Minoli, 2006, s. 5). Riziko se tedy týká statisticky předvídaného výskytu a nejistota se týká neznámé, obecně nepředvídatelné proměnné (Merna, 2007, s. 9). Nejistota je náhodná a poznávací. Náhodná vyplývá ze situace čisté náhody a poznávací je způsobena různými faktory, které vyplývají ze složitosti problému, nedostatku informací atd.

Riziko je dle Kouns, Minoli (2010, s. 43) definováno jako součin pravděpodobnosti výskytu události a dopadu této události. Merna (2007, s. 8) předkládá rozšířený model rizika, kde se riziko skládá ze čtyř základních parametrů:

- pravděpodobnost výskytu - vyjádřená jako pravděpodobnost nebo frekvence,
- závažnost dopadu při výskytu rizika – vyjádřená jako intenzita ohrožení aktiva (potenciál zničení) a průběžná změna v podmínkách nákladů a času,
- citlivost na změnu nebo externí vlivy – vyjádřená jako příležitost nebo vyrovnaný nebo nevýhodný výsledek,
- stupeň vzájemné závislosti s ostatními faktory rizika.

Nezávisle na podobě modelu poskytují modely mechanismus, pomocí kterého dochází k sdílení rizika, identifikaci, klasifikaci, další analýze a reakci na riziko. Modely vytvářejí odpověď a odhalují neuvažované faktory.

Definice rizika pro použití na informační aktivum (za předpokladu jednoduché pravděpodobnosti):

Riziko(Hrozba, Aktivum) = p(Hrozba, Aktivum).OcekavanaZtrata(Aktivum)

kde:

- *p(Hrozba, Aktivum)* – pravděpodobnost výskytu hrozby pro aktivum,
- *Hrozba* – exogenní nepříznivá situace, aktivita, náhodná událost vyvolaná zranitelností, která může způsobit poškození aktiva s pravděpodobností výskytu v dané oblasti > 0,
- *Aktivum* – předmět ochrany,

- *OcekavanaZtrata* – vyjádření poklesu hodnoty aktiva při vystavení aktiva hrozbě. U fyzických aktiv tato hodnota nepřesáhne hodnotu aktiva, u logických není shora omezena (Kouns, Minoli, 2010, s. 46).

Pro celkové riziko pak platí:

$$CelkoveRiziko = \sum_{i=1}^{z} Riziko_i(\Pr ofilHrozeb, Aktivum_i)$$

kde:

- *ProfilHrozeb* – množina všech hrozeb působících na aktivum s *p(Hrozba, Aktivum) > 0*

Očekávané ztráty souvisejících s rizikem, jsou podle Kouns, Minoli, (2010, s. 53) a Landol (2006, s. 417) vyjádřeny pomocí kvantitativních finančních měr. Typickými mírami jsou **Single Loss Expectancy** resp. **Annualized Loss Expectancy**. Platí:

$$SLE = V(A_i).EF$$

resp.

$$ALE = SLE.ARO$$

kde:

- $V(A_i)$ – hodnota aktiva vyjádřená finančně,
- *EF* (Exposition Factor) – míra poklesu hodnoty aktiva při jednotlivém výskytu kompromitace aktiva, tj. $EF(A_i) = \frac{V(A_i)_{PREDkompromitaci}}{V(A_i)_{POkompromitaci}}$,
- *ARO* (Annual Rate of Occurence) – četnost (frekvence) výskytů kompromitace aktiva za rok.

Hodnota ochranných opatření se dle Landoll (2006, s. 417) a Kouns, Minoli (2010, s. 45) vyjadřuje jako **Safeguard Value**, resp. benefit ochranných opatření a platí

$$SV = ALE_{PRED} - ALE_{PO} - ASC$$

kde:

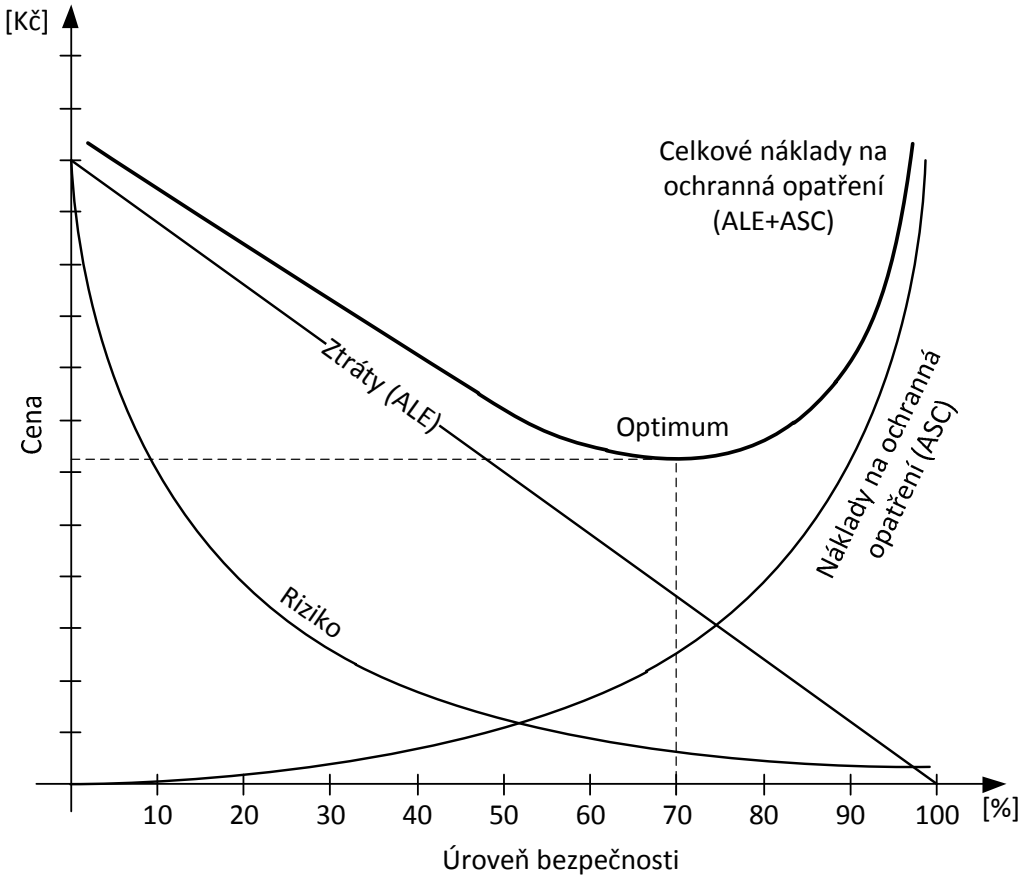
- ALE_{PRED} – očekávaná roční ztráta před (bez) aplikací protiopatření,

- ALE_{PO} – očekávaná roční ztráta po (s) aplikaci protiopatření (neboli reziduální riziko (Kouns, Minoli, 2010, s. 47)),
- ASC (Annual Safeguard Cost) – roční náklady na ochranné opatření.

Náklady na ochranná opatření jako funkce úrovně bezpečnosti vyjadřuje Graf 1. Z grafu je zřejmé, že existuje optimum mezi očekávanou ztrátou vyvolanou rizikem a cenou ochranných opatření (ASC), při kterém je v rovnováze úroveň bezpečnosti a cena bezpečnostních opatření.

Z grafu 1 je dále zřejmé, že plnou bezpečnost informací (plná eliminace rizika) nelze žádnými prostředky dosáhnout (Daler et al., 1989, s. 60). To potvrzuje i Dhillon (1997, s. 156) a Dobda (1998, s. 10, s. 23). Ideální bezpečnost informací (100 %) dle definované funkce by vyžadovala náklady, jejichž výše jde limitně do nekonečna.

Graf 1: Závislost ceny ochranných opatření na úrovni bezpečnosti



Zdroj: vlastní zpracování dle Daler (1989, s. 20); Požár (2005, s. 43); Kouns, Minoli (2010, s. 49); Doucek et al. (2011, s. 101)

Nalezení optima je cílem procesu řízení rizik a reflektuje tzv. „pragmatický směr“. Existují však situace, kdy snížení rizika má přednost před cenou opatření, např. v případech kdy jsou opatření povinná ze zákona, nebo nefinanční dopady by byly vysoké a nežádoucí (Kouns, Minoli, 2010, s. 46).

Možné metody reakce na riziko shrnuje Tabulka 3 (Smejkal, Rais, 2006, s. 112).

Tabulka 3: Metody reakce na riziko

Ztráta/Výše rizika	Vysoké riziko	Nízké riziko
Vysoká tvrdost ztráty – prudký pokles ztrátové funkce	Vyhnutí se riziku, redukce rizika	Pojištění
Nízká tvrdost ztráty – malý pokles ztrátové funkce	Retence a redukce rizika	Retence (zadržení) rizika

Zdroj: Smejkal, Rais (2006, s. 112)

Dle Dhillon (1997, s. 9, s. 27) je použití rizik jako nástroje bezpečnosti v organizaci znakem tzv. funkcionalistického paradigmatu upřednostňujícího regulaci (omezování) s cílem zajistit stabilitu a soudržnost společnosti (systému). Existující alternativní paradigmata (interpretativismus, radikálně humanistický, radikálně strukturální) připouštějí radikální změny porušující status quo. V literatuře bylo identifikováno několik osamocených pokusů prolomit „tunelové“ funkcionalistické vidění a při řešení bezpečnosti přejít k alternativním paradigmatům, nicméně dominující je nadále funkcionalistické (Dhillon, 1997, s. 28, s. 156).

Tato práce vychází z funkcionalistického paradigmatu s využitím tradičního přístupů rizik a zaměřuje se na oblast redukce rizika.

4. 4 Rizika a hrozby pro informační aktiva

Bezpečnostní riziko je pravděpodobnost, s jakou bude hodnota aktiva zničena nebo poškozena působením konkrétní hrozby při využití zranitelnosti (slabé stránky) (Požár, 2005, s. 37; Landoll, 2006, s. 34; Dobda, 1998, s. 14).

Zdroji rizik jsou dle kap. 4. 3 výhradně hrozby a související útočníci. Ke klasifikaci hrozby pro informační aktiva v této práci autor využívá vícerozměrnou klasifikaci dle Jouini et al. (2014, s. 492). Zde jsou hrozby klasifikovány:

- podle zdroje hrozby (threat source) – interní a externí (perspektiva organizační i individuální),
- podle útočníka (threat agent) – zahrnuje 3 třídy: člověk, prostředí a technologie,
- podle motivace hrozby (threat motivation) – podvodná nebo nepodvodná,
- podle záměru hrozby (threat intention) – záměrná nebo náhodná,
- podle dopadu hrozby (threat impact) – zničení informace, poškození informace, krádež/ztráta informace, zveřejnění informace, nemožnost použít informaci, zpřístupnění informace a nepovolené použití (Jouini et al., 2014, s. 492).

Z konkrétních identifikovaných reálných případů uskutečnění hrozeb lze uvést obecně **lidský faktor**, kde nepodvodné náhodné hrozbě vystavuje např. nízké povědomí o informačních rizicích a podlehnutí sociálnímu inženýrství, podvodnými záměrnými hrozbami pak jsou cílené krádeže obchodního tajemství, osobních informací a intelektuálního vlastnictví, dále případy obchodu s interními informacemi způsobené subfaktorem „insider traiding“ a případy mezinárodní špionáže. Faktorem úspěchu podvodné záměrné hrozby je zvyšující se efektivita útočníků a rostoucí komplexita jejich nástrojů (virů, mallwarů, spamů apod.). **Technologickými** hrozbami různého druhu jsou pak rozvíjející se informační infrastruktura (lokální i bezdrátové sítě, mobilní připojení a mobilní technologie), vzájemné globální propojení informačních systémů (internet) a distribuované zpracování, komunikační kanály (e-mail, www, sociální sítě) apod.

Útočníky vyplývajícími **z prostředí** jsou primárně přírodní pohromy (požáry, záplavy, zemětřesení apod.).

Pro účely této práce je podstatný závěr Jouini et al. (2014, s. 493) z něhož se dále v práci vychází. Nezávisle na zdroji, útočníkovi, motivaci, či záměru hrozby může jakákoliv kombinace těchto tříd vyústit v kterýkoliv z dopadů hrozby. Konkrétní dopad hrozby tedy není výhradním důsledkem jedné konkrétní kombinace tříd a nelze tedy univerzálně některou kombinaci vyloučit pro konkrétní dopad a omezit tak množství kombinací tříd. Tato skutečnost potvrzuje univerzálnost rozšířeného bezpečnostního modelu využívaného pro hodnocení a uvedeného v kap. 4. 5.

4. 5 Bezpečnost informací jako produkt

Bezpečností informace se dle obecné definice pojmu bezpečnost a v kontextu informace jako předmětu posuzování rozumí kvalita resp. stav, který vyjadřuje míru zachování kritických charakteristik informace. Zajištění potřebné míry kritických charakteristik informací je dosahováno prostředky ochrany těchto charakteristik (ČSN ISO/IEC 27000 in Doucek et al., 2011, s. 55). Bezpečnost informace je v této práci chápána jako produkt procesů řízení informační bezpečnosti a bezpečnostní pozice informačního systému.

Zdroje (ISO/IEC 17799, 2006; ČSN ISO/IEC 27002, 2008; Smejkal, Rais, 2006, s. 198; Požár, 2005, s. 46; Whitman, 2010, s. 6; Kouns, Minoli, 2010, s. 6 ad.) jednoznačně pracují s modelem zahrnujícím tři základní kritické charakteristiky informací. Těmito charakteristikami jsou **důvěrnost** (angl. confidentiality), **integrita** (angl. integrity) a **dostupnost** (angl. availability). Uvedené charakteristiky jsou všeobecně označovány jako C.I.A. triáda.

Model základních kritických charakteristik je dále rozšířen o kritické charakteristiky a procesy (CNSS in Whitman, 2012, s. 6). Jedná se o **soukromí** (angl. privacy), neodmítnutelnost odpovědnosti (angl. accountability) a procesy identifikace (angl. identification), autentizace (angl. authentication) a autorizace (angl. authorization) (také dle ČSN ISO/IEC 27002 (2008) nazývané priority). Důvodem rozšíření modelu základních kritických charakteristik je konstantní rozvoj specifických hrozeb (Whitman, 2010, s. 6). Neodmítnutelnost odpovědnosti a doplňkové procesy jsou zřejmým nástrojem eliminace hrozeb a snižování rizik, které přímo nebo nepřímo působí na základní kritické charakteristiky. Jedná se tedy o protiopatření.

Oproti CNSS in Whitman (2010, s. 5) vyčleňuje Herrmann (2012, s. 10) a Doucek et al. (2011, s. 83) soukromí na úroveň pojmu bezpečnost a posuzuje ji jako samostatnou charakteristiku. Důvodem je skutečnost, že soukromí je chápáno jako zákonem regulované právo jedince na ochranu charakteristik (skutečností) jeho života a možnost vlastní kontroly informací. Nejedná se o technickou disciplínu (Herrmann, 2012, s. 11; Daler, 1989, s. 17). Soukromí je předmětem samostatné rodiny norem ISO/IEC 29000, což taktéž vystihuje samostatnou povahu této charakteristiky. Technická disciplína je prostředkem zajištění, že zákonná práva na soukromí jsou

zajišťována v souladu se zákonem a organizačními politikami. Kvalita soukromí je přímo či nepřímo závislá na ostatních bezpečnostních charakteristikách (Herrmann, 2012, s. 351) a je neformální motivací pro aplikaci bezpečnosti informací (Doucek et al., 2011, s. 83).

Peltier (2002, s. 110) nahlíží na kritické charakteristiky informací při jejich posuzování ze dvou perspektiv. Jedná se o **citlivost** (angl. sensitivity, potřeba pro důvěrnost, integritu a kontrolované užití) a **dostupnost** (informace je dostupná právě v okamžiku potřeby).

Porušení kritických charakteristik informací mají následující dopady:

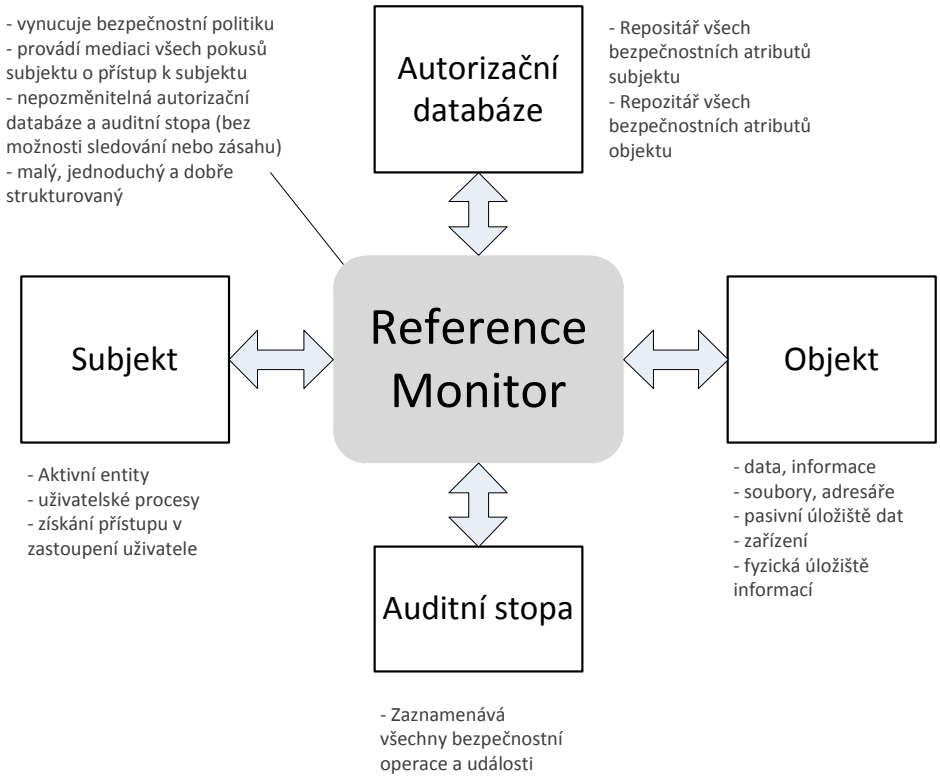
- Důvěrnost - Pokud informace postrádá tuto charakteristiku, může být dostupná i těm subjektům, které nejsou oprávněny mít k ní přístup (Dobda, 1998, s. 17). Zveřejněná důvěrná informace může porušit soukromí jednotlivců i celků, omezit organizační konkurenční výhodu nebo může způsobit organizaci škodu (Peltier, 2002, s. 111).
- Integrita - pokud postrádá informace tuto charakteristiku, může být změněná nebo zničená, úmyslně nebo neúmyslně (Dobda, 1998, s. 17).
- Dostupnost - pokud postrádá informace tuto charakteristiku, může být v určitém okamžiku nedostupná všem, nebo někomu, kteří jsou oprávněni mít k ní přístup (Dobda, 1998, s. 17).

Kritické charakteristiky informací v relaci s životním cyklem informace zohledňuje CNSS model (Whitman, 2010, s. 5). Výsledkem je trojrozměrná matice daná relací
(Důvěrnost, Integrita, Dostupnost) x (Uložení, Zpracování, Přenos) x (Politika, Vzdělávání, Technologie).

Pro popis vlastností systému bezpečně zpracovávajícího informace (ve smyslu zachování důvěrnosti a integrity informací) byl v roce 1972 panelem deseti průmyslových, vládních a akademických expertů pod vedením J. P. Andersona vyvinut koncept **„Reference Monitoru“**, který je abstraktním strojem pro mediaci přístupu subjektů (aktivních entit, uživatelů) k objektům (datům, zprávám, zařízením).

Reference Monitor je považován za referenční koncept bezpečného systému. Přestože se jedná o letitý koncept, je nadále součástí odborných vzdělávacích kurzů a je využíván pro definici vlastností a funkčností systému, které zajišťují kritické bezpečnostní charakteristiky informace. Tato skutečnost se odrazila v kritériích pro bezpečné informační systémy stanovených americkou vládou v normě TCSEC (DOD, 1985, s. 64), resp. v národním standardu ITSEC (DOTAI, 1991, s. 33). Koncept Reference Monitoru je implementován kombinací hardware a software (Anderson, 1972, s. 17). Model Reference Monitoru je uveden ve Schéma 4.

Schéma 4: Koncept Reference Monitoru



Zdroj: přeloženo autorem dle Anderson (1972, s. 17), Gutmann (2004, s. 49)

kde:

Objekt – chráněný objekt, informační aktivum

Subjekt – aktivní entita

Autorizační databáze –bezpečnostní model realizující politiku přístupu

Auditní stopa – auditní záznamy operací realizovaných Reference Monitorem

Reference Monitor – abstraktní stroj podle Anderson (1972)

Platí, že implementací mechanismu validace reference v souladu s Reference Monitorem budou všechny přístupy k objektům odpovídat politice řízení přístupu (Tilborg et al. 2011, s. 1038). To platí za splnění požadavků na Reference Monitor:

1) **úplná mediace**, kdy mechanismus validace reference zprostředkovává všechny bezpečnostně sensitivní operace, nelze jej obejít a je vždy vyvolán,
2) **nemodifikovatelnost** (angl. tamperproof), kdy subjekt nemůže modifikovat validační mechanismus,
3) **verifikovatelnost mechanismu**, kdy implementace musí být takového rozsahu, aby bylo možno verifikovat její správnost s ohledem na realizované cíle.

Pokud platí, že obecný systém realizuje mechanismus validace reference za splnění výše uvedených požadavků (obsahuje tzv. bezpečnostní jádro nebo sadu bezpečnostně relevantních komponent, angl. Security Kernel), zakládá tím důvěryhodnou výpočetní základnu (angl. Trusted Computing Base, dále TCB) (DOD, 1985, s. 65; DOTAI, 1991, s. 9) v níž platí, že odchylka reálné sady bezpečnostních požadavků oproti nastavené množině bezpečnostních požadavků je minimalizována. Bezpečnostní požadavky mají za cíl zachování hodnoty objektu, tedy aby rizika pro objekty byla minimalizována.

V současnosti identifikované bezpečnostní požadavky jsou v literatuře jednotně klasifikovány do tříd. Zdroje ISO 27002:2008 in Doucek (2011, s. 135), Whitman (2010, s. 213), Požár (2005, s. 101) resp. Zák. 412/2005 Sb. o ochraně osobních údajů jednotně uvádějí třídy opatření:

Řízení přístupu (RIZ_PRISTUP) – je prvek řízení informační bezpečnosti s podstatným vlivem na kritické charakteristiky informací (Whitman, 2010, s. 213). Dle Požár (2005, s. 101) je součástí politiky přístupu k zabezpečení informačních a komunikačních systémů. Řízení přístupu uživatelů do chráněných oblastí, ať už logický přístup k počítačovým informačním systémům, případně i fyzický přístup k zařízením a prostředkům. Předpokladem je, že každá fyzická osoba v informačním systému disponuje jednoznačnou identitou. Řízení přístupu je v současnosti postaveno na hlavních principech *nejmenšího oprávnění* (least privilege; přístup mají subjekty jen

k informacím, ke kterým mají potřebu přistupovat a dále pro akce, které mají povoleno provádět, tj. číst, psát, apod.), *potřeba přístupu* (need to know; omezuje přístupy k informacím subjektům pouze pro vykonání jejich pracovního úkonu), separace odpovědností (separation of duties, princip čtyř a více očí; odpovědnost za dokončení úkolu je rozdělena mezi více subjektů, kteří pouze společně a nerozlučně mohou úkol vykonat). Whitman (2010, s. 214) uvádí další metodologie pro řízení přístupu, tj. podle jejich vlastních specifických charakteristik (preventivní, odstrašující, vyšetřovací, nápravné, zotavovací, kompenzační) a podle jejich dopadu na organizaci (řídící, provozní, technické).

Bezpečnostní klasifikace informací (KLASIF_RIZ_INF) – Pro dosažení určitého relevantního stupně bezpečnosti je třeba rozlišovat informace, které vyžadují ochranu a které ji nevyžadují. Bezpečnostní klasifikace informací je primárním mechanismem pro následnou spolehlivou aplikaci řízení přístupu. Stejně tak je klasifikace informací podstatná pro řízení informačních aktiv, které určuje, která aktiva s jakou klasifikací mohou být kde umístěna, že mají konkrétního vlastníka a jak jsou bezpečně používána (ISO 27002:2008 in Doucek, 2011, s. 136). Přístup nastavení společné úrovně bezpečnosti na nejvyšší úroveň klasifikace pro všechna data a informace je extrémně nákladný. Navíc tento přístup naráží na lidský faktor, který odmítá respektovat pravidla, pokud pro ně neshledává smysluplný důvod. Příliš vysoká klasifikace může být stejně nebezpečná jako příliš nízká klasifikace (Daler et al., 1989, s. 61). Klasifikační stupně v závislosti na organizaci zahrnují např. v modelu Bell-Lapadula modelu škálu NEKLASIFIKOVÁNO-DŮVĚRNÉ-TAJNÉ-PŘÍSNĚ TAJNÉ (Gutmann, 2004, s. 50), případně v organizačních strukturách zavedenou škálu VEŘEJNÉ-INTERNÍ-OSOBNÍ-DISKRÉTNÍ (ČZU, 2008, s. 12). Předpokládá se práce s informacemi v určité kvalitě, která odpovídá požadavkům na informace pro účely informačního procesu. Pro účely principu soukromí je dle Herrmann (2007, s. 524) součástí řízení infroačních aktiv práce s kvalitními a nezkreslenými údaji. Součástí by tedy mělo být sledování kvality informace.

Bezpečnost informačních a komunikačních systémů (TECH_BEZP) – zahrnuje míru bezpečnosti implementace v technických zařízeních. S použitím formálních modelů jsou technická zařízení, politiky a postupy označeny podle úrovně

jejich schopnosti zajistit kritické charakteristiky informací. Formální modely jsou popsány tzv. úrovněmi záruky podle definovaného standardu, typicky Common Criteria, resp. TCSEC, ITSEC, Bell-LaPadula Confidentiality Model, Biba integrity model, Clark Wilson Integrity Model, Graham-Denning Access Control Model, Harrison-Ruzzo-Ullman Model (Whitman, 2010, s. 219). Tato oblast zapojuje principy zajištění integrity (kontrolní součty, otisky, digitální podpisy), principy zajištění důvěrnosti (kryptografie a šifrování) a obecné principy konstrukce bezpečných systémů (angl. Security Engineering). Tato kritéria byla navržena pro technická bezpečnostní opatření implementovaná v hardware, software, a firmware, nicméně částečně se dotýkají netechnických aspektů typu postupů pro osoby, fyzickou bezpečnost a bezpečnost postupů, pouze však ve vztahu k technickým opatřením.

Fyzická bezpečnost a bezpečnost prostředí (FYZ_BEZP) – zahrnuje bezpečnost zařízení ve smyslu fyzického umístění, neporušitelnosti zdroje energie, omezení možnosti rušení a odposlechu apod. (ISO 27002:2008 in Doucek, 2011, s. 141).

Akvizice, vývoj a údržba informačních systémů (AK_VY_UDR) – zahrnuje opatření spojená se SW aplikacemi (rozvojem, nasazením a údržbou), které jako primární prostředek řízení životního cyklu informací je kritickým bezpečnostním místem informačního systému (ISO 27002:2008 in Doucek, 2011, s. 147).

Personální bezpečnost, bezpečnost z pohledu lidských zdrojů (PERS_BEZP) – zahrnuje stanovení odpovědností pracovníků, jejich primární identifikaci, vytváření motivace k dodržování bezpečnostních pravidel a sankční postihy v případě prohřešků (ISO 27002:2008 in Doucek, 2011, s. 140). Tato oblast tvoří vstup pro řízení přístupu.

Zajištění kontinuity činností organizace (KONT_CINN) – zaměřuje se na zachování části kritické charakteristiky informací – dostupnost, která je z velké části závislá na spolehlivosti provozu informačních systémů.

4. 6 Bezpečnost informací jako produkt kontinuity činností

Třída opatření pro zajištění kontinuity činností organizace a provozu informačních systémů (**KONT_CINN)** má vliv především na kritickou charakteristiku informace –

dostupnost, ovlivňuje však i ostatní kritické charakteristiky informace prostřednictvím vyřazení činnosti některého prvku informačního systému, jehož účelovou funkcí je ochrana. Pak může být narušena schopnost informačního systému zajistit důvěrnost, integritu a dostupnost (plnit roli Reference Monitoru). S ohledem na kritickou závislost organizace na trvalé dostupnosti informací by jednou z priorit organizace měla být trvalá spolehlivost provozu informačního systému prostředky řízení kontinuity činností.

Podle výzkumu Urbancová et al. (2013), který se zaměřuje na organizace v České republice, patří mezi nejčastější příčiny událostí, které organizace v rámci kontinuity činností řeší a které mají největší dopad na organizaci, technologické chyby hardwaru a softwaru (30 %), ztráty klíčových pracovníků a znalostí (25 %), přírodní pohromy a epidemie (20 %), neúmyslné lidské chyby (10 %) a úmyslné lidské chyby (10 %). U 5 % organizací nelze příčiny událostí, které mají největší dopad na organizaci, stanovit, jelikož organizace nemá k dispozici analýzu rizik.

Zavedení procesu zajištění kontinuity činností včetně případné certifikace a auditu je dlouhodobý proces, 55 % organizacím trvalo zavedení systematického zajištění kontinuity činností do organizačních procesů více než 12 měsíců, 40 % organizacím 6 až 12 měsíců a 5 % organizacím méně než 6 měsíců.

81,1 % organizací, které nezabezpečují kontinuitu své činnosti, uvádělo jako důvody nezabezpečení nejčastěji skutečnost, že neshledávají kontinuitu činnosti organizace důležitou (66,3 %), dále finanční důvody, tj. zejména vysokou cenu (16,3 %), neexistující podporu ze strany managementu organizace (11,6 %) a nedostatek kvalifikovaných pracovníků (9,3 %). Kontinuitu činnosti nejčastěji neshledávají důležitým malé (59,6 %) a střední organizace (35,1 %). 20,9 % organizací, které se v současné době problematice nevěnují, uvedlo, že uvažují o zavedení kontinuity činnosti v časovém horizontu 5 let.

Z uvedeného vyplývá, že kontinuita činností jako vlivná třída opatření pro zachování kritických charakteristik informace je v českých organizacích podceňována a lze očekávat nižší bezpečnostní kvalitu informačních systémů primárně v oblasti kritické charakteristiky dostupnosti. Pro zachování úrovně bezpečnosti informací lze však tuto část charakteristiky delegovat na externě poskytované systémy a soustředit se na kritické charakteristiky informace důvěrnosti a integrity.

4. 7 Bezpečnost informací a soukromí z pohledu legislativy

Problematika soukromí, bezpečnosti informací a ochrany dat vyžaduje jednotný právní rámec a to buď regionálně lokální, případně globální. Legislativa definuje vztahy mezi informacemi, jejich majiteli, organizacemi a případnými narušiteli a dalšími subjekty vstupujícími do vztahu s informacemi. Cílem legislativy je primárně na základě etických pravidel kodifikovat očekávaná pravidla chování společnosti (Whitman, 2010, s. 429) a dát možnost postihnout narušení legálních vztahů jinými subjekty a tato narušení postihovat za účelem regulace narušení a ochrany oprávněných (Dobda, 1998, s. 156). Zákony upravují informační procesy a vytvářejí transparentní ekonomické prostředí, současně pak ukládají povinnosti institucím a právním subjektům (Doucek et al., 2011, s. 185).

Vývoj legislativy vztahující se k informacím o osobách historicky začal v USA, kde se na základě různých iniciativ a úřadů prosadily a dle Herrmann (2007, s. 154-365) postupně vyvinuly zákony „Computer Security Act“ (dnes Public Law 100-235), Gramm-Leach-Bliley Act (GBL), Sarbanes-Oxley Act (SOX) ve finančním průmyslu, Health Insurance Portability and Accounting Act (HIPAA), Personal Health Information Act (PHIA) ve zdravotnictví, Personal Information Protection and Electronic Document Act (PIPEDA), Privacy Act a Patriot Act. Tyto zákony mají za cíl omezit nesprávné nakládání, zneužití a zpronevěru citlivých informací (Herrmann, 2007, s. 351). Dalšími obecnými zákony jsou Security and Freedom through Encryption Act (Whitman, 2010, s. 439), Freedom of Information Act (Whitman, 2010, s. 440), které řeší export informací z USA.

V rámci Evropské legislativy byla nejprve ve Švédsku, v Německu a v Rakousku a dále na celoevropské úrovni Radou Evropy definována „Úmluva na ochranu osob se zřetelem na automatizované zpracování osobních údajů“ (Doucek et al., 2011, s. 190). Následovaly zákony Data Protection Directive (Evropská komise) a Data Protection Act (Velká Británie) (Herrmann, 2007, s. 351).

Hlavním účelem uvedených zákonů je postihnout rámce legálního nakládání s informacemi fyzických osob, organizací za účelem ochrany soukromí osob a obchodních zájmů ekonomických celků.

Základní aktuálně platný legislativní rámec ve vztahu k bezpečnosti informací je v České republice tvořen především zákony a vyhláškami a dále institucemi, které na základě těchto zákonů vznikají a jejichž působnost je zákony definována. Hlavními zákony jsou Zákon č. 101/2000 Sb. o ochraně osobních údajů, Zákon č. 106/1999 Sb. o svobodném přístupu k informacím, Zákon č. 240/2000 Sb. o krizovém řízení, Zákon č. 365/2000 Sb. o informačních systémech veřejné správy, Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, Zákon č. 121/2000 Sb. Autorský zákon a Zákon č. 181/2014 Sb. o kybernetické bezpečnosti. Významným prostředkem pro posílení elektronické komunikace občanů nejen se státní správou, ale i ve veřejném a soukromém sektoru byl Zákon 227/2000 Sb. o elektronickém podpisu.

Na základě zákonů jsou pak zřizovány úřady nebo zavazovány instituce. Hlavními působícími institucemi je nezávislý Úřad na ochranu osobních údajů (ÚOOÚ), vzniklý na základě Zákona 101/2000 Sb., Národní bezpečnostní úřad (NBÚ) působící na základě zákona 412/2005 Sb., Ministerstvo vnitra, které mimo jiné působí a zajišťuje výkon vybraných kompetencí podle zákona 365/2000 Sb.

Mimo tyto oficiální instituce působí v České republice nezávislá sdružení typu Iuridicum Remedium zaměřující se kriticky na organizace porušující soukromí jednotlivce a ochranu osobních údajů a další.

V Evropské unii je významné působení agentury ENISA, Evropské agentury pro síťovou a informační bezpečnost. ENISA byla spuštěna s cílem rozšířit schopnost EU, členských států a obchodních komunit předcházet, vyjadřovat se a reagovat na síťové a informační bezpečnostní problémy. ENISA je poradní orgán, zpracovatel dat o bezpečnostních incidentech, podporovatel principů hodnocení rizik a spolupráce při zvyšování povědomí o bezpečnosti informací (ENISA, 2015).

Novým prvkem v legislativě ČR je Zákon 181/2014 Sb. o kybernetické bezpečnosti a související Vyhláška č. 316/2014 Sb. o kybernetické bezpečnosti, resp. Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích a dalších změnách v souvisejících zákonech, primárně souvisejících s tzv. kritickou infrastrukturou. Cílem zákona je umožnit státu reagovat na krizové situace v kybernetickém světě a je nástrojem národní strategie kyberbezpečnosti. Zákon je v zemích EU jedním z prvních zákonů zastřešujících a uvádějících od 1. 1. 2015 do

praxe oblast kybernetické bezpečnosti. Realizátorem je NBÚ ve spolupráci s vybranými státními a soukromými subjekty a Národním centrem kybernetické bezpečnosti (CERT). Zákon je postaven na pilířích: ISO 27000, identifikace incidentů a procesech hlášení a zvládnutí těchto incidentů prostřednictvím CERT. Zákon zavádí pojmy „Kybernetický prostor“, „Kritická informační infrastruktura“, „Kritická komunikační infrastruktura“, „Správce informačního systému“, „Bezpečnost informací a bezpečnostní opatření“ ad. Pro cíl této práce je podstatné, že zavedená terminologie je v souladu s terminologií zákona a téma práce předkládá možný nástroj pro vybudování bezpečnostně robustnějších informačních systémů podle tohoto zákona.

Zákony, vyhlášky a instituce vytvářejí legislativní rámec České republiky a jsou nástrojem transformace společnosti (definují pravidla společnosti) a transformace ekonomiky. Cílem je udržovat soulad s legislativou Evropské unie a kompatibilitu s globálně prosazovanými pravidly s využitím mechanismů harmonizace.

4. 8 Disciplína informační bezpečnosti

Informační bezpečnost je disciplína zabývající se prostředky pro dosažení cíle – bezpečnosti informací, tedy jak z definice bezpečnosti informací vyplývá, zajištění kritických charakteristik informací a dosažení stavu, kdy jsou informace ochráněny před ztrátou těchto kritických charakteristik. To potvrzuje Doucek et al. (2011, s. 47). Disciplína informační bezpečnosti zahrnuje množinu mechanismů, technik, měr a administrativních procesů využívaných k ochraně informačních aktiv (Kouns, Minoli, 2010, s. 3), tedy ochranu investic vložených do informací a informačních systémů (Doucek et al., 2011, s. 185).

Informační bezpečnost je jednou ze součástí bezpečnostního systému organizace (Smejkal, Rais, 2006, s. 195), resp. celkové bezpečnosti organizace (Doucek et al., 2011, s. 56; Požár, 2005, s. 39).

Informační bezpečnost řeší veškerou ochranu informací organizace, tedy celého informačního systému, automatizované i neautomatizované části (v mluvené, v psané formě, při zpracování a přenosu, tedy při používání telefonů, faxů, prostřednictvím telekomunikační sítě) (Smejkal, Rais, 2006, s. 197), uložení a správu archivu

nedigitálních dat, skartace materiálů, nakládání s nimi během transportu, publikace informací do médií apod. (Doucek et al., 2011, s. 56).

Bezpečnost informací v informačním systému je dosahována bezpečností informačních systémů podporovaných prostředky informačních a komunikačních technologií.

4. 9 Metody a systémy řízení informační bezpečnosti

Principy zajišťování bezpečnosti informací se rozvíjely historicky v různých podobách díky různým úhlům pohledu na problematiku a byly motivovány především oborovými specifiky a inspirované poznáním skutečností a procesů v daném oboru. Vývoj řízení bezpečnosti informací probíhal ve vývojových vlnách – technické (1960-1980), manažerské (1980-1995), institucionální (1995-2000) a vlny správy a řízení (2000-nyní) (Von Solms, 2006, s. 165). V aktuální vlně správy a řízení je bezpečnost informací institucionalizována a začleněna jako integrální součást podnikové správy a řízení (Enterprise Governance) a má pevnou vazbu na Správu a řízení informačních technologií (IT Governance) (Doucek et al., 2011, s. 36). To především znamená, že bezpečnost informací je teoreticky zpracovaná oblast postavená na obecných principech a promítnutá v obecných standardech, pomocí kterých může správa a řízení probíhat.

Žádoucími výstupy správy a řízení bezpečnosti informací je dle Doucek et al. (2011, s. 37) udržení vazby mezi bezpečností informací a strategií organizace, řízení informačních rizik a řízení zdrojů, hodnocení realizace cílů informační bezpečnosti pomocí měření, monitorování a reportingu a vykazování dosažených hodnot pomocí optimalizace investic do bezpečnosti informací. Základní cíle informační bezpečnosti jsou splněny, pokud je zachována dostupnost, důvěrnost, integrita a nepopiratelnost původu informací (Doucek et al., 2011, s. 40), tedy kritické charakteristiky informací.

Řízení informačních rizik se zaměřuje na ochranu informací před jejich možnou ztrátou nebo poškozením ve smyslu kritických charakteristik informací. Obecně se kvality ochrany dosahuje tím, že jsou určena aktiva resp. informace, která se mají chránit, a řízena možná rizika snižující bezpečnost těchto aktiv resp. informací (Smejkal, Rais, 2006, s. 103).

Smejkal, Rais (2006, s. 201) shrnuje podstatné fáze budování informační bezpečnosti do čtyř etap:

- Analýza informačních rizik a případná klasifikace informací – zde dochází k identifikaci aktiv, stanovení hodnoty aktiv a souvisejících rizikových atributů aktiv (Smejkal, Rais, 2006, s. 81). Analýza rizik se provádí v rozsahu celého informačního systému (Požár, 2005, s. 87). Při aplikaci moderních přístupů jsou zjištěná rizika evidována v registru rizik, který současně umožňuje aktualizaci a zajišťuje komunikaci hodnot rizik (Doucek et al., 2011, s. 95).
- Příprava bezpečnostní politiky organizace - politiky definují cíle s použitím obecných výrazů. Jedná se o vyjádření organizačních cílů směrem k určité oblasti zájmu. Standardy pak specifikují, co v kontextu politiky musí být splněno. Postupy definují, jak dosáhnout standardu (Peltier, 2002, s. 27). Efektivní a smysluplné politiky vyžadují podpůrné prostředky. Politiky neposkytují uživatelské komunitě dostatečné vedení k její implementaci a splnění cíle organizace. K poskytnutí podpory a vedení slouží standardy. Standardy zahrnují povinné aktivity, akce, pravidla nebo omezení vytvořené pro podporu politik. Standardy jsou velmi často finančně náročné na správu, a proto jsou aplikovány uváženě (Peltier, 2002, s. 27).
- Vytvoření příslušných organizačních struktur (bezpečnostní management) a interních právních norem (bezpečnostních předpisů).
- Realizace bezpečnostních opatření formou bezpečnostních projektů.
- Testování bezpečnostního systému a provoz zahrnující reakci na bezpečnostní incidenty.

Moderní postup dosahování bezpečnosti informací je obecně postaven na Demmingově iteračním principu zdokonalování procesů PDCA (Plan-Do-Check-Act), který aplikuje především norma ISO/IEC 27001.

Jednotlivé fáze v cyklu PDCA jsou rozděleny následovně:

- Ustanovení systému řízení bezpečnosti informací (Plan) – dle ISO/IEC 27001 in Whitman (2010, s. 229) a Doucek et al. (2011, s. 96) zahrnuje činnosti definice rozsahu, politiky systému řízení bezpečnosti informací, analýza rizik a způsob jejich zvládání vč. akceptace zbytkových rizik, a prohlášení o aplikovatelnosti.
- Zavádění a provoz systému řízení bezpečnosti informací (Do) - dle ISO/IEC 27001 in Whitman (2010, s. 229) a Doucek et al. (2011, s. 111) zahrnuje přípravu plánu zvládání rizik a zavedení bezpečnostních opatření včetně příručky bezpečnosti informací, definovat program zaměřený na povědomí lidských zdrojů a odborných pracovníků bezpečnosti, implementace postupů k detekci a reakci na bezpečnostní incidenty, řídit zdroje a formální základnu systému řízení bezpečnosti informací.
- Monitorování a přezkoumávání systému řízení bezpečnosti informací (Check) - dle ISO/IEC 27001 in Whitman (2010, s. 229) a Doucek et al. (2011, s. 123) zahrnuje monitorování a ověření účinnosti prosazování bezpečnostních opatření, provádění interních auditů, příprava zprávy o zjištěných výsledcích fáze včetně revize zbytkových a akceptovaných rizik, přehodnocení stavu z pohledu vedení. Z pohledu systému se jedná o zpětnou vazbu procesu umožňující korekci a optimalizaci postupů.
- Údržba a zlepšování systému řízení bezpečnosti informací (Act) - dle ISO/IEC 27001 in Whitman (2010, s. 229) a Doucek et al. (2011, s. 125) zahrnuje činnosti zavádění identifikovaných možností zlepšení či provádění odpovídajících opatření k nápravě a preventivních opatření, komunikace výsledků zájmovým skupinám.

Volba modelu řízení bezpečnosti a odpovídajících metod závisí na podmínkách a potřebách organizace a jejím zaměření. V průběhu vývoje disciplíny informační bezpečnosti postupně vznikla množina modelů řízení a standardů, které jsou volně použitelné, případně proprietární. V českých podmínkách aplikovanou množinu modelů sumarizuje Tabulka 4.

Tabulka 4: Množina modelů a standardů řízení informační bezpečnosti

Model, standard	Zaměření	Obsah standardu
Rodina standardů (ČSN) ISO/IEC 27000 (navazuje na ISO 17799 a BS 7799)	Univerzální standard řízení informační bezpečnosti	Nejvíce odkazovaný bezpečnostní model. Zaměřuje se vytvoření společné základny pro spuštění, implementaci a údržbu bezpečnosti v organizaci. (Whitman, 2010, s. 227), tedy systém řízení informační bezpečnosti. Hlavním přínosem normy je harmonizace přístupů a obsah vydávaných norem. Norma zahrnuje části (rozlišené samotným číslem normy), tj. přehled a slovník, požadavky, soubor postupů, směrnici zavádění ISMS, měření, řízení rizik, požadavky na orgány auditu a certifikaci, audit a další. Zaměřuje se nejen na obecné postupy, ale též na odvětvová specifika, tj. komunikace mezi organizacemi, telekomunikace, zdravotnictví, finanční služby, organizační ekonomika apod.
(ČSN) ISO/IEC 13335	Standard bezpečnosti informačních technologií (IT)	Sestává ze 4 hlavních částí se zaměřením na pojetí a modely bezpečnosti IT, Řízení a plánování, Techniky pro řízení, výběr ochranných opatření. Je určen pro manažery bezpečnosti IT.
NIST SP 800	Standard řízení informační bezpečnosti	Poskytuje v porovnání s ISO 27000 jinou strukturu řízení informační bezpečnosti a je více prosazována americkou vládou především z důvodů volné dostupnosti a má delší historii, tedy prošla důkladnější revizí vládou a profesionály (Whitman, 2010, s. 228). Míry se primárně zaměřují na bezpečnostní politiky a procesy, jejich efektivitu a dopady do obchodní sféry.
ITIL (IT infrastructure library)	Metodika poskytování služeb IT	Mezinárodně uznávaný procesně orientovaný standard aktuálně ve verzi 3 poskytující množinu metod a „best practices“ pro řízení vývoje a provozu infrastruktur informačních systémů. ITIL se soustřeďuje na plánování, vývoj, modifikaci, dodávku, správu, analýzu a použití IT. Jednou ze součástí je řízení informační bezpečnosti s cílem propojení informační bezpečnosti s celkovou bezpečností organizace.
COBIT (Control Objectives for Information and related technology)	Metodika pro systematické řízení informačních a komunikačních technologií (ICT)	Jedná se o sadu všeobecně přijímaných procesů, návodů, ukazatelů a „best practices“ s cílem maximalizovat užitek z ICT. Cíle COBIT jsou rozděleny do několika oblastí: plánování a organizování, akvizice a implementace, dodání a podpora, monitorování a hodnocení (Doucek et al., 2011, s. 43). Dává velmi dobrý základ pro řízení operačních rizik (Whitman, 2010, s. 237) podle cílových skupin (domácí uživatelé, vedoucí, exekutiva, nejvyšší vedení, statutární orgány) (Doucek et al., 2011, s. 47). COBIT ve verzi 5 (2012) obsahuje část speciálně orientovanou na kvalitativní cíle informační bezpečnosti, řízení rizik, požadavky na služby, architekturu a hodnocení plnění cílů.

Zdroj: vlastní zpracování

Společným rysem uvedených standardů je komplexní realizace cíle disciplíny informační bezpečnosti. Přístupy k řízení se do jisté míry liší a mezi standardy dochází k vzájemné harmonizaci při zachování účelu daného standardu. Součástí každého standardu je však vždy fáze zajišťující kontrolu plnění cílů a nastavení nápravných opatření tak, aby docházelo k vylepšení výsledků konkrétního procesu.

4. 10 Modelové přístupy k řízení informační bezpečnosti

Doucek et al. (2011, s. 131) uvádí modelové přístupy organizací k řízení informační bezpečnosti. Modelový přístup přímo určuje úroveň aplikace metod řízení informační bezpečnosti:

- Model ignorativní bezpečnosti – ochrana informací není zohledňována. Je typický pro mikroorganizace, které se zaměřují na vlastní rozvoj obchodu.
- Model minimální technologické bezpečnosti – bezpečnost informací je chápána jako jedna ze služeb provozu informačních systémů. Jedná se o organizace, kde bezpečnost informací není rozvinuta na strategické ani taktické úrovni. Model odpovídá přístupu organizací z 80-tých let minulého století.
- Model formální bezpečnosti – organizace se řízením bezpečnosti zabývá formálně, role manažera podnikové informatiky je formálně spojena s manažerem informační bezpečnosti.
- Model odtržené bezpečnosti – řízení informační bezpečnosti není součástí provozu informačních systémů, ale je řešena samostatnou rolí, která je zařazena do vrcholového vedení organizace.
- Model utopené bezpečnosti – řízení informační bezpečnosti je podřízeno řízení informatiky. Model je typický pro 75 % organizací v ČR.
- Model agilní bezpečnosti – typická pro velké organizace, kdy všeobecnou bezpečnost organizace řeší samostatná rada zodpovědná za správu aktiv organizace.
- Model institucionální bezpečnosti – typická pro rozsáhlé organizace, kde rada pro bezpečnost je rozdělena na obecnou bezpečnost a bezpečnost IS/ICT.

Je zřejmé, že organizace budou aplikovat konkrétní model (tj. přistupovat k informační bezpečnosti) v závislosti na perspektivách, vyplývajících především z priorit organizace (orientace zájmových skupin) a organizační kultury (Hayden, 2010, s. 277).

Identifikované perspektivy bezpečnosti informací:

- Ekonomická (finanční) – bezpečnost je vždy zvažována z pohledu finančního. Bezpečnostní a nápravné mechanismy, vybavení, strategie a rozhodnutí jsou vždy řízenými finančními podmínkami (Kouns, Minoli, 2010, s. 53). Je zde jasná vazba na aplikování pragmatického směru aplikace řízení rizik (viz kap. 4. 3). Investice do ochranných opatření je vždy zvažována z pohledu návratnosti.
- Personální – vypovídá o zaměření na hloubku bezpečnostního povědomí uživatelů (zaměstnanců, klientů), lidské zdroje či procento času stráveného na aktivitách řešících bezpečnost informačního systému. Lidský faktor je vždy součástí informačního systému, povědomí lidí o hrozbách a způsobech boje proti nim je významný faktor (Peltier, 2010, s. 158).
- Technická – vypovídá o zaměření na provoz informačních systémů (Doucek et al., 2011, s. 110), provoz v perimetru, např. počet propuštěných a zadržených emailových zpráv, počtu nainstalovaných trezorů, antivirových ochran a firewallů (Jaquith, 2007, s. 47), životnost bezpečnostní technologie (Dobda, 1998, s. 31), síle nasazených kryptografických ochran, maximální dobu dostupnosti informačního systému (Hayden, 2010, s. 278) apod. se schopností flexibilně a rychle reagovat na problémy, resp. obchodní potřeby bez narušení ostatních procesů.
- Kvalitativní (bezpečnostní) – vypovídá o zaměření na dosaženou míru bezpečnosti informací v informačním systému ve smyslu kritických charakteristik informací a souvisejících oblastí, tj. důvěrnost, integrita, dostupnost, ochrana proti ztrátě dat, vývoj bezpečného programového vybavení apod. Míry mohou stanovit pravděpodobnost hrozby, identifikovat nové zranitelnosti, zhodnotit pokrytí protiopatřeními, účinnost protiopatření, mohou identifikovat trendy a navrhnout „best practices“, míry vypracované nad historickými daty mohou být použity pro plánování a reakci (Jaquith, 2007, s. 241).
- Soulad s legislativou a standardy – vypovídá o zaměření na soulad s bezpečnostními politikami a legislativou (Jaquith, 2007, s. 241).

Použití konkrétních tříd a nahlížení na informační systémy z uvedených perspektiv je závislé na konkrétních podmínkách organizace (velikosti, finančních možnostech) a na možnostech sběru dat potřebných pro výpočty.

Efektivita procesů řízení bezpečnosti informací v organizaci je hodnocena podle schopnosti realizovat cíle informační bezpečnosti (perspektiva bezpečnostní, zachování kritických charakteristik informací). Faktorem, který tuto efektivitu primárně ovlivňuje je požadavek být optimální z perspektivy ekonomické (z pohledu nákladů na mitigaci rizik a eliminace zranitelností) při zachování souladu s externími regulacemi.

4. 11 Kvantitativní hodnocení bezpečnosti informací

Nástrojem pro kvantitativní hodnocení je proces měření (angl. measurement). Cílem měření je získání objektivních dat pro podporu procesu rozhodování. Měření a rozhodování probíhá na základě specifikovaných měr (angl. measures).

V řídících procesech organizace má měření na základě měr následující přínosy:

- pomáhá určovat priority, o něž by měla organizace usilovat při maximalizaci své přidané hodnoty (Učeň, 2001, s. 36; Doucek, 2011, s. 108),
- umožňuje zdokonalování ekonomických parametrů procesů (snížení nákladů, zvyšování zisku, růst produktivity, zkracování doby životního cyklu) (Doucek, 2011, s. 108),
- indikuje aktivity a procesy, které nemají přidanou hodnotu (Doucek, 2011, s. 108),
- garantuje rovnováhu při naplňování dlouhodobých, střednědobých a krátkodobých cílů (Učeň, 2001, s. 36; Doucek, 2011, s. 108).

Míry mají průřezový charakter, tj. přiřazení míry k dané oblasti slouží jako nástroj pro systemizaci míry (Učeň, 2001, s. 38), a současně vypovídají o dalších souvisejících problémových oblastech, případně tyto související oblasti přímo ovlivňují (tedy např. měření procesů řízení informační bezpečnosti ovlivní jak bezpečnost informací, tak kvalitu software a jiné problémové oblasti).

Brotby (2010), Herrman (2010), Jaquith (2007), Hayden (2010) a existující standardy zaměřující se na měření bezpečnosti informací a efektivitu řízení informační bezpečnosti (ISO/IEC 27004, NIST SP 800-55 (SP 800-80), ISO/IEC 27033 1-5) se liší v pohledu na přístup k hodnocení. Standardy poskytují široké spektrum indikátorů, které lze rozdělit do skupiny finanční, personální a technické (Doucek et al., 2010). Není však ustálená taxonomie jednotlivých měr, což obecně vychází z různého chápání a posuzování bezpečnosti a informační bezpečnosti z různých perspektiv. Zřejmým důvodem je rozdělení vnímání pojmů „bezpečnost“, „informační bezpečnost“ a „informační zajištění“ (Brotby, 2009, s. 16). Stav hodnocení v rámci uvedených norem měření sumarizuje Doucek et al. (2011, s. 109). Další zdroje (Jaquith, 2007; Brotby, 2010; Hayden, 2010; Herrmann, 2010) se detailně zabývají procesy a postupy měření a konkrétními mírami, odkud vyplývají požadavky aplikované při stanovování měr:

- nemělo by se jednat jen o finanční ukazatele, ale měla by být zajištěna jejich provázanost na finanční a hodnototvorný systém, tj. uplatnit vyvážený poměr tvrdých a měkkých měr,
- je možné je zpracovávat pomocí matematicko-statistických metod,
- jsou objektivně měřitelné, resp. objektivizovatelné v případě subjektivních měr (Doucek et al., 2011, s. 115),
- jsou opakovatelné,
- jsou nezávislé na čase měření,
- nemusí být uváděny nutně v absolutních hodnotách, v určitých situacích dostačuje možnost relativního srovnání s referenční hodnotou (Doucek et al., 2011, s. 115),
- jsou objektivně interpretovatelné, resp. objektivní (Brotby, 2010, s. 16),
- jsou optimální z pohledu nákladů a přínosů měření,
- mají účel, který je dle Brotby (2010, s. 18) definován jako sada kvalitativních faktorů: předmět měření, cíl měření, postup, průběh měření, časové a prostorové podmínky měření, subjekt měření (zájmová skupina), interpretace výsledků a jejich význam pro cílový subjekt.

Obecně jsou míry kategorizovány podle:

- předmětu měření – procesy, výkon, výstupy, kvalitu, trendy (Brotby, 2010, s. 15),
- metod měření – vícerozměrné skórovací karty, hodnoty, benchmarking, modelování, statistická analýza, resp. jejich kombinace. Je podstatné rozlišovat, zda metoda generuje kvantitativní výstupy a do jaké míry spolehlivě generuje přesný kvantitativní popis bezpečnostních cílů (Venderel, 2008, s. 2).

Podle ISO/IEC 15939 in Vaníček (2004, s. 153) se rozlišují základní a odvozené míry. Základní míry vychází přímo z reality, lze je snímat přímým pozorováním nebo experimentálně. Odvozené míry se ze základních vytvářejí užitím funkcí a matematických operací. Míry měří stav měřitelných fyzických nebo abstraktních vlastností měřených objektů – atributů. Jeden atribut je součástí více podcharakteristik, resp. charakteristik, což znamená rozšíření vlivu tohoto atributu na jiné podcharakteristiky a nutnost s touto skutečností pracovat v hodnocení.

Aktuálně publikované konstrukty měření sumarizuje Tabulka 5. V souladu s cílem práce žádný ze standardů neposkytuje návod na stanovování a výběr adekvátních měr bezpečnosti informací (Heinzle et al., 2013, s. 88, 94).

Tabulka 5: Modely měření bezpečnosti a orientace na měření

Model, standard	**Orientace na hodnocení metodou měření**	**Reference na standard**
Rodina standardů (ČSN) ISO/IEC 27000	ANO	ISO/IEC 27004, ISO/IEC 27033 1-5
NIST SP 800	ANO	SP 800-55, SP 800-80
COBIT	ANO	COBIT 5 (2012)
The CIS Security Metrics (The Center for Internet Security, 2010)	ANO	-
Security metametrics blog (Brotby et al., 2013)	ANO	-

Zdroj: Heinzle et al. (2013, s. 89), doplněno autorem o české normy

Proces měření definovaný v ISO 27004 vychází z principu sledování stanovených bezpečnostních cílů a opatření stanovených na základě analýzy rizik, které jsou následně implementovány, a je měřena jejich efektivnost, čímž je prokazováno dosažení požadované úrovně dosažení bezpečnostních cílů. Míra dosažení požadované úrovně následně slouží pro naplnění informačních potřeb v procesu řízení.

Konstrukt měření bezpečnosti informací definovaný v normě definuje údaje identifikující a popisující sledované míry. Soubor údajů míry zahrnuje tyto údaje (ISO 27004, 2009, s. 22):

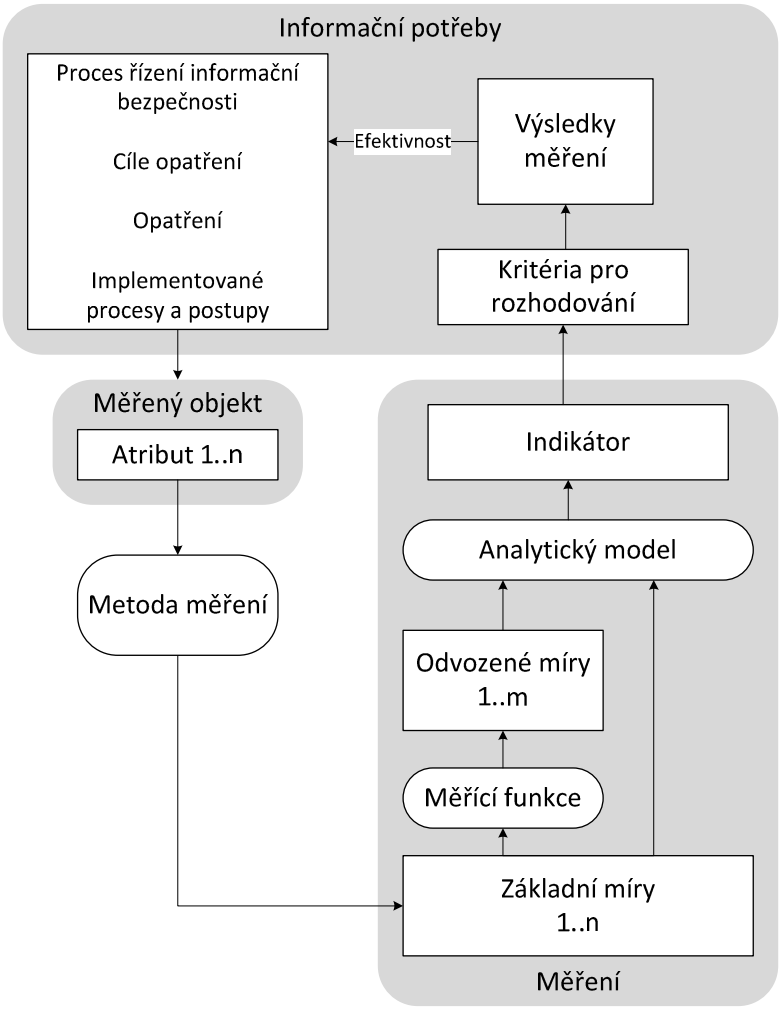
- identifikační údaje sledované míry,
- identifikační údaje měřeného objektu a jeho měřené atributy,
- parametry základních měr 1..n,
- seznam odvozených měr a asociovanou měřicí funkci použitou pro odvození,
- specifikace indikátoru a popis analytické funkce pro odvození indikátoru,
- specifikaci kritérií pro rozhodování,
- interpretaci indikátorů a způsob reportování,
- frekvenci provádění měření a vyhodnocení,
- identifikaci zájmových skupin.

Vaníček (2004, s. 157) shodně s ISO/IEC 9126 identifikuje následující doplňkové údaje k výše uvedeným, které lze využít:

- typ měřicí stupnice,
- místo měření,
- charakteristiky a podcharakteristiky podstatně ovlivněné mírou,
- druh míry (vnitřní, vnější, v užití).

Samotný proces měření pak probíhá podle modelu měření informační bezpečnosti uvedeného v Schéma 5.

Schéma 5: Model měření informační bezpečnosti dle ISO 27004



Zdroj: přeloženo a překlesleno autorem dle ISO 27004:2009 (2009, s. 7)

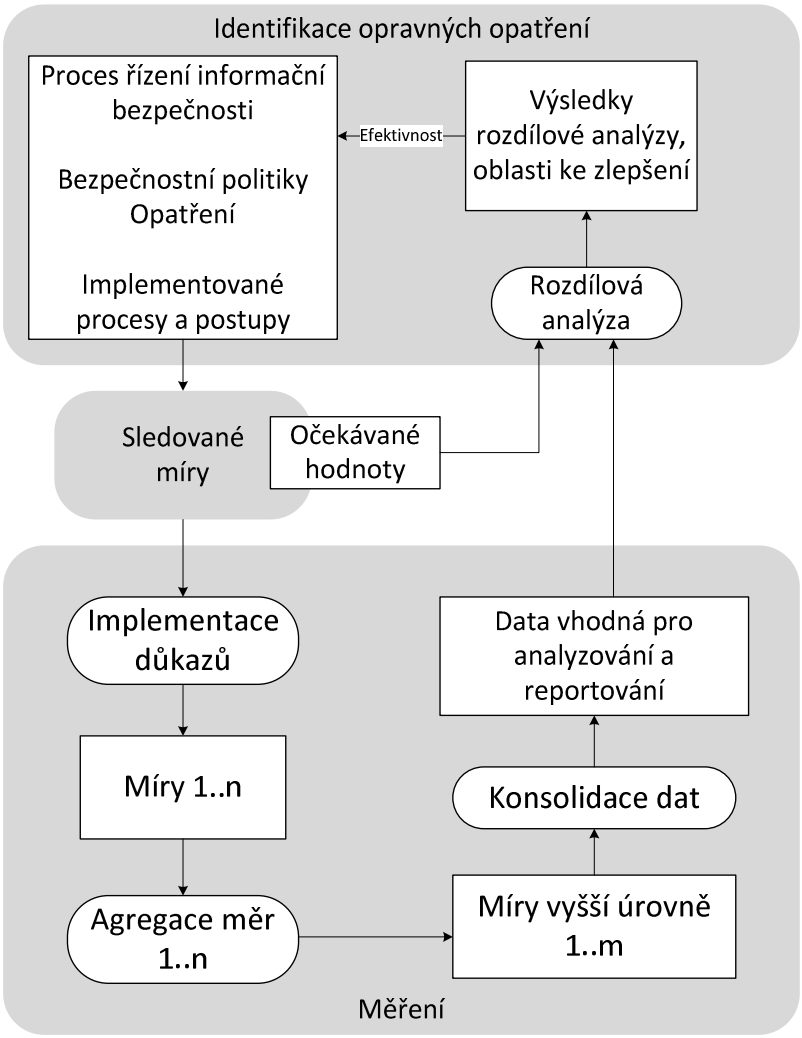
Proces měření definovaný v NIST SP 800-55 je obecněji zaměřený, sleduje efektivnost bezpečnostních politik a bezpečnostních procesů a dopady do obchodní sféry. Konstrukt měření bezpečnosti informací v normě definuje následující soubor údajů míry (NIST SP800-55, 2008, s. 31):

- identifikační údaje sledované míry,
- cíl měření rozlišený podle úrovně míry (systémová nebo programová),
- definice míry vycházející z kontrolních opatření a typ míry (implementační, míra efektivnosti, míra dopadu),
- způsob výpočtu celkové numerické hodnoty na základě změřených hodnot (lze považovat za analytický model),

- cílový rozsah míry, který je považován za uspokojivý (lze považovat za definici indikátoru),
- technika měření (implementace důkazů),
- frekvence měření,
- identifikace zdroje měr,
- způsob reportování,
- identifikaci zájmových skupin.

Samotný proces měření je pak popsán sekvencí kroků popsaných v Schéma 6.

Schéma 6: Model měření informační bezpečnosti dle NIST SP 800-55



Zdroj: přeloženo a překresleno autorem dle NIST SP 800-55 (2008, s. 44)

Vytvoření obecné míry má dle Jaquith (2007, s. 244, 246) vývojový charakter, který prochází revidovacím procesem. Klíčové kroky vývojového procesu míry jsou:

- identifikace míry,
- definice míry,
- vývoj míry,
- zajištění kvality,
- nasazení míry,
- vizualizace výsledků,
- analýza výsledků,
- publikace výsledků.

Jednotlivé kroky umožňují různý stupeň automatizace (Jaquith, 2007, s. 245).

Proces vytvoření konkrétních měr orientovaných na bezpečnost informací je závislý na schopnosti identifikovat konkrétní míru, charakteristiky a atributy. Cíle a míry závisí na perspektivě a potřebách zájmové skupiny, která výsledky vyhodnocuje. Jeden cíl bude mít zřejmě vývojový pracovník a jiný cíl bude mít manažer konfigurace, nebo Chief Information Officer. Lze však předpokládat, že za jednotlivými záměry je společný cíl, požadovaná úroveň bezpečnosti informací a záruk.

Literatura uvádí různé **metody identifikace měr**. Brotby (2013, s. 46), Herrmann (2007, s. 46) a Hayden (2010, s. 52) zmiňují primárně GQM přístup, Brotby (2010, s. 47) pak doplňuje CMM (Capability Maturity Model), který definuje sérii pěti úrovní popisující společné postupy, které jsou charakteristické pro určitou úroveň.

GQM (Goal-Question-Metric) reprezentuje systematický přístup k provázání a zapojení cílů do modelů programovacích procesů, produktů a zájmů kvality založených na potřebách projektů a organizací (Basili et al., 1994a, s. 528). Metoda GQM zahrnuje tři kroky:

1) identifikace cíle na konceptuální úrovni (v závislosti na zájmové skupině),
2) identifikace otázek vztahujících se ke konkrétním komponentám a aktivitám, které slouží k dosažení cílů na provozní úrovni,
3) identifikace měr (objektivních nebo subjektivních), které pokryjí otázky.

GQM je hierarchická struktura s kořenem v Cíli (Goal). Cíl je upřesněn do několika otázek (Q) a každá otázka dekomponuje oblast do hlavních komponent. Každá otázka je následně dekomponována na odpovídající míry. Jedna míra může odpovídat na různé otázky v několika cílích (Basili et al., 1994a, s. 529).

Výsledkem aplikace GQM je zaměření na konkrétní množinu oblastí a množinu pravidel pro interpretaci změřených dat. Principem GQM je orientace měření na splnění cíle. Strukturovaným procesem GQM lze identifikovat konkrétní míry logickým a strukturovaným (top-down) procesem (Hayden, 2010, s. 52; Herrmann, 2007, s. 22) zmiňovaným taktéž v Brotby et al. (2013, s. 46). Související aktivity obsahují stanovení měřených charakteristik a stanovení analytického modelu společně se stanovením referenčních hodnot, tj. vytvoření konstruktu míry. Top-down přístup umožňuje definovat předmět měření, který by měl být měřen, zatímco alternativní přístup bottom-up je postaven na reálných možnostech měření a vychází ze snadno měřitelných množin charakteristik.

Kritéria pro akceptaci míry zavádí Brotby et al. (2013) pomocí popisu míry a jejího zhodnocení pomocí měr druhé úrovně (míry měr, metametriky) se sadou kritérií, které vypovídají o míře – predikceschopná, relevantní, akceschopná, původní, smysluplná, přesná, aktuální, nezávislá, nákladově přiměřená. Tento přístup je označován jako PRAGMATIC. Přístup nazvaný „Validace proveditelnosti míry“ (angl. Security Metrics Feasibility Validation) směřující k většímu cílovému množství kritérií definuje Savola (2010, s. 234) a zavádí 3 stupně realizovatelnosti míry: důvěryhodnost, aplikovatelnost, dostatečnost. Každý stupeň zahrnuje další charakteristiky. Ve výsledku je dle Savola (2010, s. 235) nutno pokrýt a vyhodnotit prioritu 19-ti charakteristik míry, než je míra akceptována. Tento proces je v porovnání s PRAGMATIC metodou náročnější a lze očekávat, že bude narážet na překážky při aplikaci.

Lze shrnout, že pokrytí životního cyklu míry není triviální a dle dostupné literatury jeho složitost odpovídá realizačnímu projektu menšího rozsahu. Základními kritickými kroky je **identifikace měr vhodnou metodou**, **vývoj** a **nasazení míry do procesu měření** a **zajištění kvality měření a sběr výsledků**. Podstatnou fází je **prezentace výstupů měření** pro uspokojení informačních potřeb zájmových skupin a promítnutí získaných indikátorů do organizačních procesů.

4. 12 Průzkum způsobů hodnocení aplikovaných v současné praxi

Pro zjištění způsobů hodnocení bezpečnosti informačních systémů aplikovaných v současné praxi byl realizován průzkum, který napomohl k identifikaci a ověření bílých míst v současné teorii a praxi a potvrzení hlavního a dílčích cílů disertační práce. Průzkum byl realizován formou rozhovorů se 3 manažery informační bezpečnosti ve třech organizacích v ČR (organizace A, B a C). Původní názvy organizací byly na žádost zástupců anonymizovány.

Výběr organizací proběhl podle následujících kritérií:

- sektor organizace: finanční sektor,
- velikost organizace: velká organizace nad 250 zaměstnanců v ČR,
- zpracování hodnotných informací zaměstnanců a klientů v informačním systému organizace,
- systém řízení informační bezpečnosti: na bázi ISO 27000, optimálně certifikace,
- modelový přístup k řízení informační bezpečnosti: model utopené nebo odtržené bezpečnosti (viz kap. 4. 10).

Průzkum probíhal od 3. 6. 2013 do 7. 6. 2013.

Zástupce organizace A uvedl, že v rámci procesů řízení informační bezpečnosti jsou klasifikovány informační systémy podle kritičnosti. Kritičnost je primárně posuzována podle jejich významu pro obchodní činnost a z pohledu externích regulací a legislativy. Identifikace kritických systémů probíhá na základě dotazníků a dále kvalitativním způsobem na základě rozhovorů s garanty aplikací.

V organizaci jsou vytvořeny formální postupy pro posouzení bezpečnosti informací a jsou využívány systémy pro monitoring anomálního chování uživatelů (porušení bezpečnostní politiky, přístupy privilegovanými účty) a úroveň zabezpečení technických prostředků v provozu je sledována kontinuální analýzou zranitelností. Provozované aplikace podléhají testování bezpečnosti externím subjektem. Použité techniky jsou založeny na kvalitativním hodnocení. Zástupce uvedl, že jsou sledovány údaje ze sledovaných systémů, k jejichž sběru lze použít standardizované softwarové

nástroje. Není zpětná vazba na požadovanou úroveň rizika. Analytické modely využívají základních statistických technik – sledování četností a aritmetických průměrů. Neexistuje způsob, jak ověřit, že uvedené hodnoty vyjadřují úroveň bezpečnosti informací. Konkrétní konstrukt pro měření charakteristik informačního systému podle konkrétního standardu není v organizaci aplikován.

Zástupce organizace B uvedl, že hodnocení informačních systémů z pohledu bezpečnosti je realizováno primárně ve fázi návrhu a konstrukce systému a následně prověřováno externími subjekty. V provozu dochází k základnímu sledování provozu a aplikačních žurnálů, primárně tedy provozní monitoring. Kvantitativní hodnocení není aplikováno, úroveň bezpečnosti informací a snižování rizik je dosahováno prosazováním bezpečnostní politiky, tj. konfigurací pracovních stanic a minimalizací počtu nepovolených operací globální bezpečnostní politikou a dále školením uživatelů metodou e-learningu. Korporátní politika pro hodnocení bezpečnosti informací a jednotný systémový přístup pro agregaci evidovaných údajů není stanovena, měření a vyhodnocení konkrétního systému nebo oddělení není prioritou a není zřejmé, že by přispělo k výraznému snížení rizika. Z pohledu vedení jsou podstatné trendy zjišťovaných charakteristik a dopad na obchodní činnost organizace.

Zástupce organizace C uvedl, že v organizaci je pro hodnocení bezpečnosti informací zřízeno pracoviště bezpečnostního monitoringu, které vyhodnocuje detekované incidenty. Pracoviště zaměstnává skupinu operátorů, kteří definovaným postupem reagují na výskyt incidentu. Současně existuje skupina analytiků, kteří provádí hlubší analýzu nerozpoznaných incidentů. Zdroji údajů pro monitoring jsou provozní aplikační žurnály, databázová komunikace, pravidelně sbírané provozní systémové informace z provozních systémů, které jsou zasílány do centrálního monitoringu a přímo porovnávány s referenčními hodnotami. Referenční hodnoty jsou stanovovány iterativním způsobem na základě srovnání s předchozím stavem. Sbírané statistické údaje jsou zpracovávány základními matematicko-statistickými metodami (četnosti, odchylky). Exaktní hodnocení informačních systémů jako celku není realizováno, v kritických součástech systému jsou používány komponenty, které jsou již zhodnoceny. Kvantifikace úspěšnosti procesu řízení informační bezpečnosti spočívá v sledování trendu v časových řadách odhalených incidentů základního typu na

sledovaných systémech. Incidenty primárně znamenají porušení bezpečnostní politiky. Sledování je aplikováno plošně na všechny systémy. Konkrétní konstrukt pro měření charakteristik informačního systému podle konkrétního standardu není v organizaci aplikován.

Respondenti A a C přiznávají, že některé používané metody k vyhodnocení nasbíraných údajů nejsou vlivem velkého množství nasbíraných údajů efektivně vyhodnotitelné. Současně A, B a C přiznává, že ne vždy jsou informační aktiva katalogizovaná i s uvedenou klasifikací.

Výsledek průzkumu ve třech organizacích ve finančním sektoru, tedy v organizacích s výborně rozvinutou oblastí informační bezpečnosti, ukazuje, že aplikované principy kvantitativního hodnocení se soustředí na monitoring vybraných událostí a detekce porušení bezpečnostní politiky. Aplikace měření na základě stanovených měr a využívání vhodných statistických metod pro hodnocení úrovně bezpečnosti informací na základě konkrétního modelu na bázi ISO 27004, které by prokazovalo snížení rizika pro zpracovávané informace vlivem aplikace konkrétních opatření, nebyla identifikována.

Deklarovaná nevhodnost některých metod měření indikuje neexistenci vhodného analytického modelu. Důsledkem je, že v konkrétních oblastech nejsou respondenti schopni prokazovat aplikaci a účinnost bezpečnostních opatření na žádoucí úrovni. Systematický postup vývoje a použití měr stanovených na základě specifického vlastního resp. normativního konstruktu měření respondenti nevyužívají. Nutno podotknout, že technika monitorování neposkytuje vhodné kvantitativní hodnoty pro proces měření a nelze jej tedy s procesem měření slučovat.

Na základě průzkumu v organizacích A, B, C a přímého pozorování byl pro účely této práce autorem vytvořen zobecněný model chování organizace (Schéma 7) a byl verifikován se zástupci organizací. Byla zavedena zobecněná terminologie, neboť jednotlivé fáze, procesy a výstupy jsou v jednotlivých organizacích pojmenovány různě (např. Model chování organizace k riziku zahrnuje „B: Risk Tolerance“, „C: Risk Apetit“, „B: Security Risk Posture“, „A: Executive Data Sponsor“, „A: Data processor“

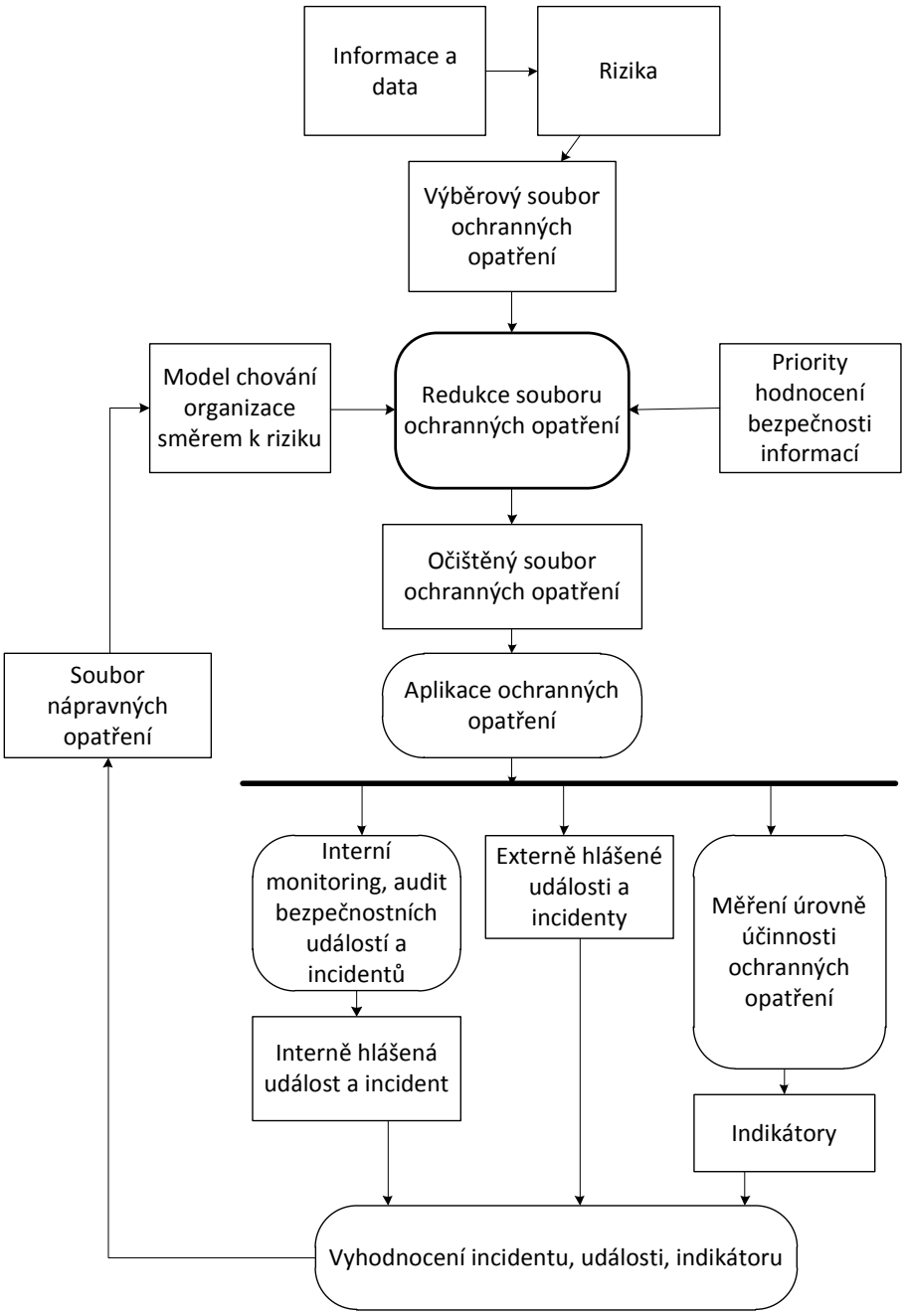
apod.). Konkrétní názvy nemohou být v práci uvedeny, protože jsou ve všech organizacích klasifikovány jako důvěrné.

Jednotlivé aktivity v modelu jsou realizovány v různých podobách na operativní, taktické i strategické úrovni a s různými časovými odstupy. Výstupy aktivit v modelu jsou v organizacích revidovány a v modelu kopírují cyklus PDCA (viz kap. 4. 9). Jednotlivé fáze cyklu jsou pokryty takto:

- Plan – zahrnuje identifikaci informačních aktiv a rizik, redukci výběrového souboru ochranných opatření na očištěný soubor ochranných opatření. Redukce je prováděna buď vědomě na základě strategických bezpečnostních rozhodnutí, resp. jiným způsobem (vědomě, nevědomě, cíleně).
- Do – zahrnuje aplikaci očištěného souboru ochranných opatření v definované kvalitě.
- Check – zahrnuje kontrolu provedených opatření, která je realizována v závislosti na organizačních podmínkách a modelu chování organizace směrem k riziku buď **vlastními internímí prostředky** (technikou monitoringu, auditu apod.), nebo závisí na **externě hlášených událostech a incidentech**, nebo jejich kombinací. Vybrané organizace aplikují blíže nespecifikované způsoby **měření v informačním systému** využívající blíže nespecifikované metody stanovení měr.
- Act – zahrnuje implementaci souboru nápravných opatření, které jsou realizovány s novým očištěným výběrovým souborem opatření, jehož modifikace obnáší ovlivnění modelu chování organizace směrem k riziku.

Výběrový soubor opatření je normativem definovaná množina všech opatření pro redukci rizika. Výběrový soubor je podmnožinou **základního souboru opatření**, což je teoretická množina všech opatření, které jsou aplikovatelné k dosažení maximální možné redukce rizik. **Očištěný výběrový soubor** je množina opatření aplikovaná v konkrétní organizaci a je závislá na faktorech vyplývajících primárně z podmínek organizace, tj. její ochotě akceptovat riziko pro informační aktiva (akceptace může být nevědomá), resp. prioritách v oblasti bezpečnosti informací. Účinnost aplikovaného očištěného výběrového souboru opatření je ovlivněna různými faktory.

Schéma 7: Zobecněný model chování konkrétních organizací A, B, C



Zdroj: vlastní zpracování

Zobecněný model je v další kapitole upraven do modelu s podporou měření.

5 NÁVRH MODELU A METODIKY PRO HODNOCENÍ

Dále uvedený návrh modelu a metodiky hodnocení bezpečnosti informací pokrývá dílčí cíl práce a předkládá jeden z možných přístupů pro kvantitativní hodnocení bezpečnosti informací v informačních systémech (ve smyslu kritických charakteristik informací).

5. 1 Konstrukt organizačních faktorů ovlivňujících bezpečnost informací

Na základě přehledu současného stavu řešené problematiky uvedeného v předešlých kapitolách, jehož cílem byla definice pojmů, identifikace modelů, vztahů a jejich významu v problematice bezpečnosti informací, cílů disciplíny informační bezpečnosti, aktuálního stavu vývoje disciplíny a souvisejících organizačních procesů ve světě a v České republice byl sestaven konstrukt vnitřních organizačních faktorů (Tabulka 6) ovlivňujících bezpečnost informací v informačních systémech.

Tabulka 6: Konstrukt vnitřních organizačních faktorů

Faktor	Reference	Diskutováno v kapitole
Zhodnocení závažnosti a rizik působících na informační aktiva	ISO 27005 (2004), Ouedraogo et al. (2011, s. 200)	4. 3
Zajištění ochrany kritických charakteristik informací	ČSN ISO/IEC 27000 in Doucek et al. (2011, s. 55)	4. 5
Procesy řízení informační bezpečnosti a stanovená bezpečnostní politika	ČSN ISO/IEC 27000 in Doucek et al. (2011, s. 37)	4. 8
Priority organizace v oblasti bezpečnosti informací a orientace zájmových skupin	Hayden (2010, s. 277)	4. 10
Modelový přístup organizace k řízení bezpečnosti informací	Doucek et al. (2011, s. 131)	4. 10
Měření bezpečnosti informací	ISO/IEC 27004 (2009)	4. 11
Zobecněný model chování organizací	Vlastní zpracování	4. 12

Zdroj: vlastní zpracování

Efektivita procesů řízení bezpečnosti informací v organizaci je hodnocena podle schopnosti realizovat cíle informační bezpečnosti aplikací ochranných opatření (perspektiva bezpečnostní, zachování kritických charakteristik informací). Problémem je pak získat důkazy, že efektivita těchto procesů se odráží v bezpečnostních

charakteristikách organizace jako produktu těchto procesů a nedochází k redukci ochranných opatření. Faktorem, který tuto efektivitu ovlivňuje je požadavek být optimální z perspektivy ekonomické (z pohledu nákladů na mitigaci rizik a eliminace zranitelností) při zachování souladu s externími regulacemi.

5. 2 Vliv ochranných opatření na kritické charakteristiky informace

Tato práce na základě výstupu kap. 4. 5 vychází z předpokladu, že dosahování vlastností Reference Monitoru je realizovatelné prostřednictvím implementace množiny ochranných opatření (MO_{TCB}) nad konkrétním informačním systémem.

Je zřejmé, že existuje:

1. množina MO_Z – **základní** teoretická **množina patření**, která definuje všechna opatření k pokrytí bezpečnostních požadavků, tj. k plnému dosažení všech vlastností Reference Monitoru a platí, že $MO_Z = MO_{TCB}$.
2. množina MO_V – **výběrová množina opatření**, která zahrnuje všechna doposud identifikovaná opatření a platí $MO_V \subset MO_Z$. Typicky se jedná o množinu opatření definovaných zvoleným standardem, např. ISO 27002:2009.
3. množina MO_O – **očištěná množina opatření**, která definuje reálně aplikovaná opatření na konkrétním systému a platí $MO_O \subset MO_V$. Očištění množiny MO_V na MO_O nazýváme v této práci **redukcí opatření** ovlivněné organizačními faktory (viz kap. 5. 1).
4. množina MO_N – **reziduální množina opatření**, která zahrnuje všechna opatření *O*, pro něž platí $O \in MO_Z \wedge O \notin MO_V$.

Namapováním obecných opatření MO_V na komponenty Reference Monitoru byla autorem provedena výchozí identifikace a odhad vlivu V_{TO} třídy T_O opatření $O \in MO_V$ do kritických charakteristik informace (C, I, A) (Tabulka 7).

Tabulka 7: Odhad vlivu tříd opatření na kritické charakteritistiky informace

Třída opatření/ vlastnost Reference Monitoru	**ISO 27001:2008 maska vlivu**	**Spolehlivost identifikace subjektu**	**Proveditelnost operace (CRUD) nad objektem**	**Kvalita autorizační DB**	**Proveditelnost auditování (neodmítnutelnost)**	**Výchozí odhad vlivu třídy opatření V_{TO}**
Obecné opatření	-	(+, o, -)	(-, -, o)	(+, o, o)	(o, o, o)	Max. skóre=4
RIZ_PRISTUP	(+, +, o)	(+, +, -)	(-, -, o)	**(+, +, o)**	(o, o, o)	(**2,5**; **2,5**; 1,5)
KLASIF_RIZ_INF	(+, +, +)	**(+, o, -)**	(-, -, -)	**(+, +, o)**	(o, o, o)	(**2,5**; **2**; 1)
TECH_BEZP	(+, +, +)	**(+, o, o)**	(-, -, -)	**(+, +, o)**	(-, -, -)	(**2**; **2**; 1)
FYZ_BEZP	(+, +, +)	**(+, +, o)**	(-, -, -)	**(+, +, o)**	(o, o, o)	(**2,5**;**2,5**;1,5)
AK_VY_UDR	(o, +, o)	(o, +, o)	(-, -, o)	(o, +, o)	(o, o, o)	(1,5;**2,5**;**2**)
PERS_BEZP	(+, +, +)	**(+, +, o)**	(-, -, o)	**(+, +, o)**	(o, o, o)	(**2,5**;**2,5**;**2**)
KONT_CINN	(-, -, +)	(-, -, o)	(-, -, +)	(-, -, o)	(-, -, o)	(0;0;**2,5**)
Skóre vlastnosti	Max. skóre=7	(**5,5**; **5**; 2,5)	(0; 0; 2,5)	(**5,5**; **6**; **3,5**)	(2,5; 2,5; 3)	

+ má vliv, **-** nemá vliv, **o** má částečný vliv

Souhrn vlivu tříd opatření T_O z MO_V na zachování kritických charakteristik informace a eliminaci hrozeb plynoucích ze selhání informačního systému v roli Reference Monitoru uvádí Tabulka 8. Jsou zahrnuty ty vlastnosti a ta opatření, pro která platí $Vliv(T_O) \geq \frac{Max.skóre}{2}$. Hraniční hodnoty skóre vlivu, pro které platí $Vliv(T_O) = \frac{Max.skóre}{2}$, jsou uvedeny v závorce.

Tabulka 8: Třídy opatření k dosažení bezpečnosti informací

Skupina	**Třída charakteristiky informace**	**Kritická charakteristika informace**	**Hrozba**	**Příčina**	**Třída opatření T_O**
Bezpečnost informací	Citlivost	Důvěrnost	Ztráta nebo narušení důvěrnosti, ztráta nebo únik (data loss or data leakage), tj. neautorizované čtení, porušení autorského práva, neidentifikovatelnost vlastníka	Nízká spolehlivost identifikace subjektu nebo neplatná autorizační báze, narušená proveditelnost auditování	RIZ_PRISTUP, KLASIF_RIZ_INF, (TECH_BEZP), FYZ_BEZP, PERS_BEZP
		Integrita	Ztráta integrity, tj. úmyslná nežádoucí změna dat,	Nízká spolehlivost identifikace	RIZ_PRISTUP, (KLASIF_RIZ_INF), (TECH_BEZP), FYZ_BEZP,

			neidentifikovatelnost zdroje,	subjektu nebo neplatná autorizační báze, narušená proveditelnost auditování	AK_VY_UDR, PERS_BEZP
	Dostupnost	Dostupnost	Selhání informačního systému v rámci některé fáze informačního procesu. Odmítnutí přístupu v rozporu s pravidlem NeedToKnow.	Selhání reference monitoru nebo neplatná autorizační báze nebo selhání objektu.	(AK_VY_UDR) (PERS_BEZP), KONT_CINN
Soukromí	Soukromí	Soukromí	Narušení soukromí postoupením informace k jiným účelům, než je znám vlastníkovi informace.	Vyplývají z narušení důvěrnosti nebo integrity.	(KLASIF_RIZ_INF), TECH_BEZP, PERS_BEZP RIZ_PRIST

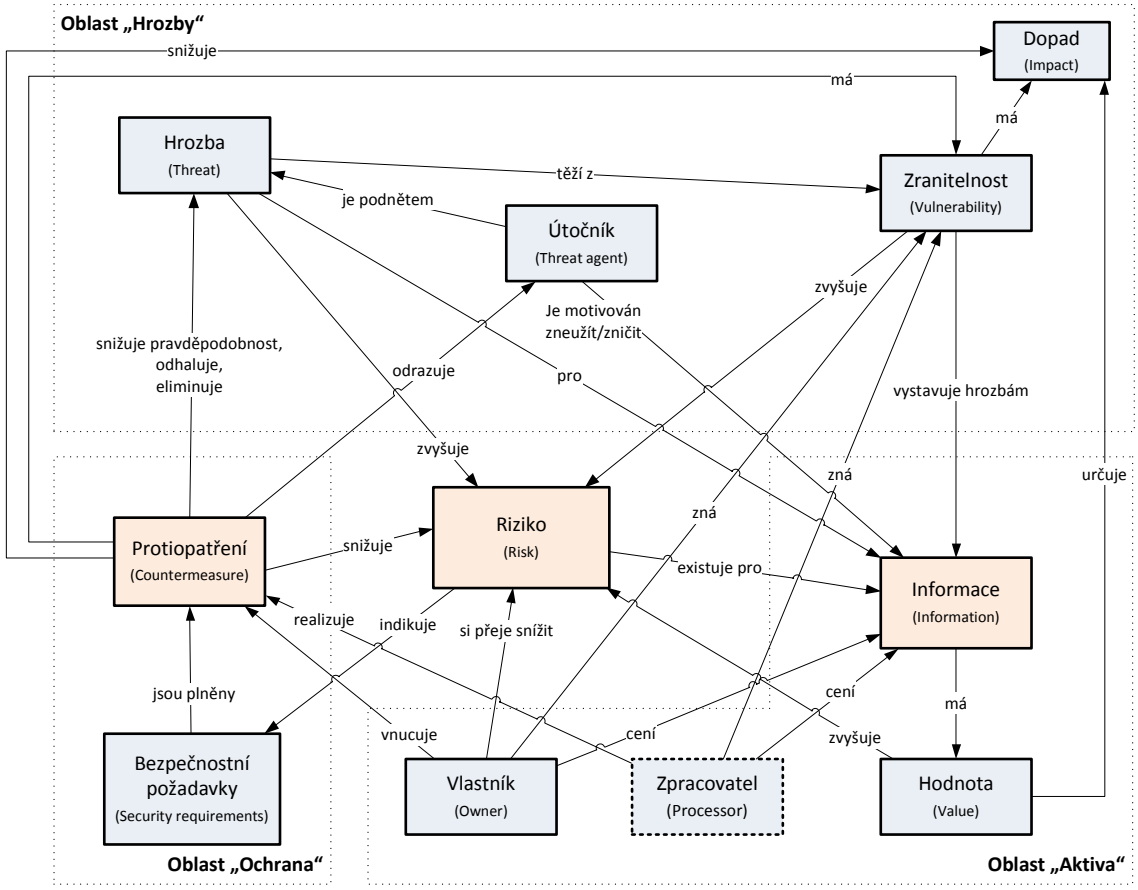
Zdroj: vlastní zpracování

Výchozí odhad vlivu a třídy ochranných opatření jsou dále použity jako nástroj pro **odhad hodnoty C, I, A** na základě jednotlivých reálně aplikovaných opatření z MO_O a jejich příslušnosti ke třídě opatření.

5. 3 Rozšířený konceptuální model bezpečnosti informací

Identifikované kritické charakteristiky informací a jejich závislost na dalších entitách shrnují jednotně Hanáček, Staudek (2000, s. 2), Smejkal, Rais (2006, s. 84), Jaquith (2007, s. 232), Kouns, Minoli (2010, s. 159), CCRA (2012, s. 39, s. 40) v konceptuálním bezpečnostním modelu. Na základě dalších zdrojů (Jouini et al., 2014) byl autorem tento model upraven do Rozšířeného konceptuálního modelu bezpečnosti informací (Schéma 8). Rozšíření autorem spočívá konkrétně v doplnění chybějící entity „Zpracovatel“ (označeno čárkovaně) a doplnění relací propojujících novou entitu s původními entitami. Cílem rozšíření je podchytit faktory v modelu, které nejsou pod kontrolou vlastníka informace.

Schéma 8: Rozšířený konceptuální model bezpečnosti informace



Zdroj: vlastní rozšířené zpracování dle Hanáček, Staudek (2000, s. 2), Smejkal, Rais (2006, s. 84), Jaquith (2007, s. 232), Kouns, Minoli (2010, s. 159), CCRA (2012, s. 39, s. 40)

Za předpokladu, že rozšířený konceptuální bezpečnostní model dle Schéma 8 je úplným, lze v oblasti bezpečnosti informací na bázi rozšířeného bezpečnostního modelu informace stanovovat cíle. Těmito cíli je obecně maximalizace účinku pozitivních relací a minimalizace účinku negativních relací. Účelem měření naplnění cílů v konkrétním okamžiku je komparace účinku relací proti referenčním nebo předchozím hodnotám nad celou množinou informací a v podmínkách konkrétního informačního systému. Lze předpokládat, že agregace okamžitých účinků relací popisuje bezpečnostní pozici informačního systému $BP_{IS}(I, t)$, soubor referenčních účinků relací popisuje cílovou referenční bezpečnostní pozici systému.

Navržená metodika pro hodnocení využívá tohoto předpokladu a rozšířený konceptuální bezpečnostní model je v rámci práce experimentálně použit jako základna

pro verifikaci stanovených cílů a otázek jako výstupů metody GQM a prostředek pro hodnocení bezpečnostní pozice systému. Charakteristiky, které byly identifikovány z rozšířeného modelu, jsou uvedeny v kap. 10. 3.

5. 4 Proces identifikace měr nástrojem GQM

GQM přístup je použit jako hlavní nástroj pro identifikaci bezpečnostních měr pro fázi návrhu metodického postupu. Top-down přístup byl zvolen jako vhodnější. Kritériem pro cílový metodický postup je použitelnost pro proces měření podle ISO 27004 podle kap. 4. 11 (výstupy jsou ve shodě s konstruktem měření podle ISO 27004:2009) a současně slučitelnost s identifikovaným konstruktem faktorů ovlivňujících bezpečnost informací. Systém měr jako výstup procesu zahrnuje konkrétní formálně popsanou identifikovanou sadu měr pro definovaný cíl při zachování kritérií pro míry.

Obecný konceptuální nástroj GQM je autorem rozšířen o verifikační fázi stanoveného cíle G, otázky Q a míry M. Verifikační fáze mají zajistit schopnost zachovat vazbu na riziko a současně na sadu bezpečnostních opatření podle zvoleného konstruktu měření, stejně jako kvalitativní parametry míry. V případě nesplnění verifikačního kritéria je zapojena korekční zpětná vazba.

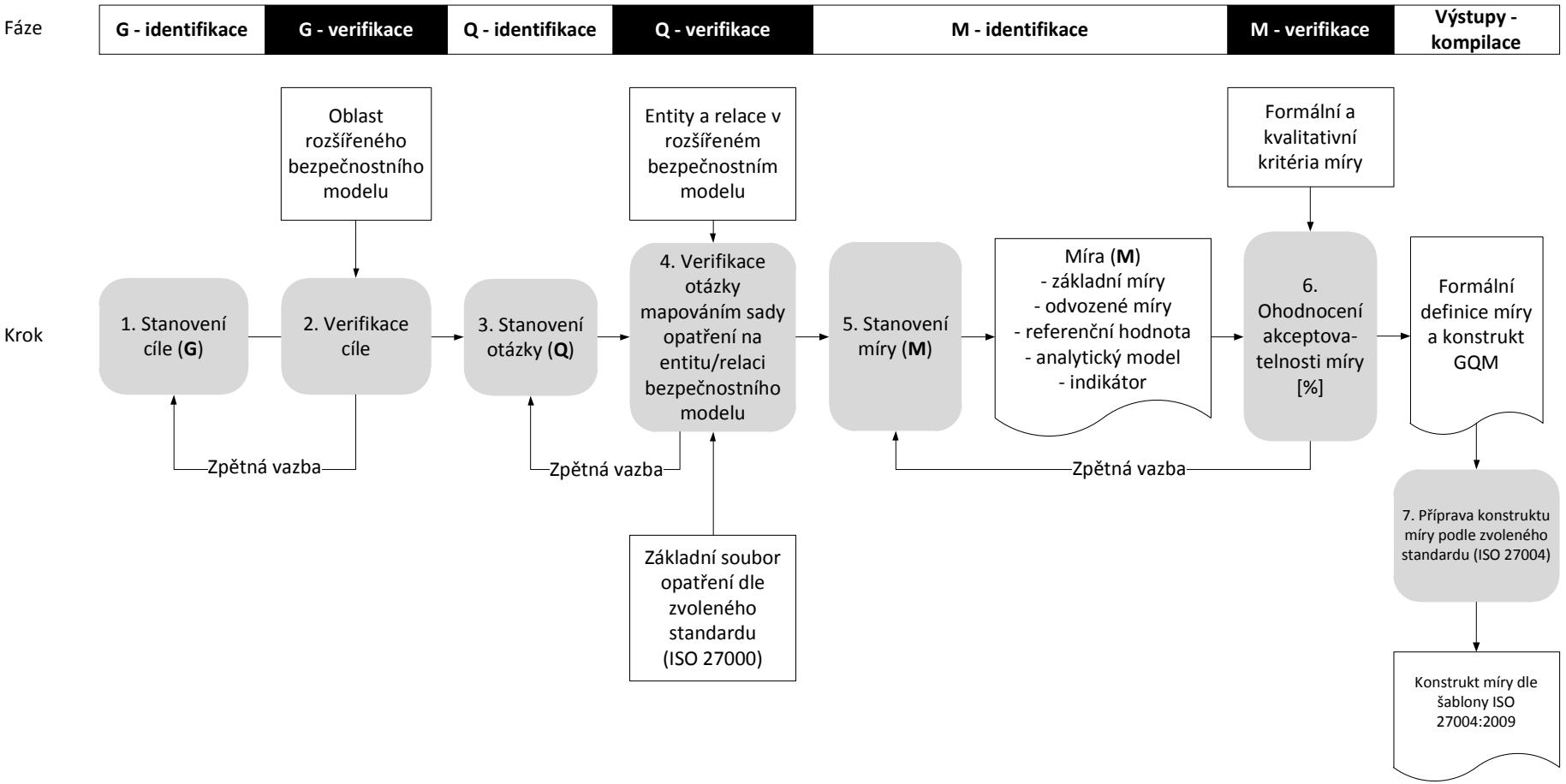
Kritériem pro výběr cíle je příslušnost k oblasti rozšířeného bezpečnostního modelu (Hrozby, Ochrana, Aktiva). Kritériem pro výběr měřitelných charakteristik a atributů předmětu měření je jednoznačná vazba na entitu nebo relaci v rozšířeném bezpečnostním modelu. Druhým kritériem je pokrytí vlastností měr uvedených v kap. 4. 11 tak, aby bylo možno vytvořit cílový konstrukt měření podle GQM (vlastní návrh konstruktu) a následně ISO 27004 (konstrukt převzat), tedy primárně stanovení předmětu měření, techniky měření a analytického modelu. Třetím kritériem je akceptovatelnost míry.

S ohledem na hierarchičnost GQM probíhají definiční fáze Q a M v iteracích, tj.:

- pro pokrytí definice otázek $Q_{1..m}$ jsou *m*-krát opakovány kroky 3 až 6,
- pro pokrytí definice měr $M_{1..n}$ jsou *n*-krát opakovány kroky 5 a 6.

Celkový postup vývoje sady měr nástrojem GQM s verifikačními fázemi shrnuje Schéma 9.

Schéma 9: Postup vývoje sady měr pomocí nástroje GQM



Zdroj: vlastní zpracování

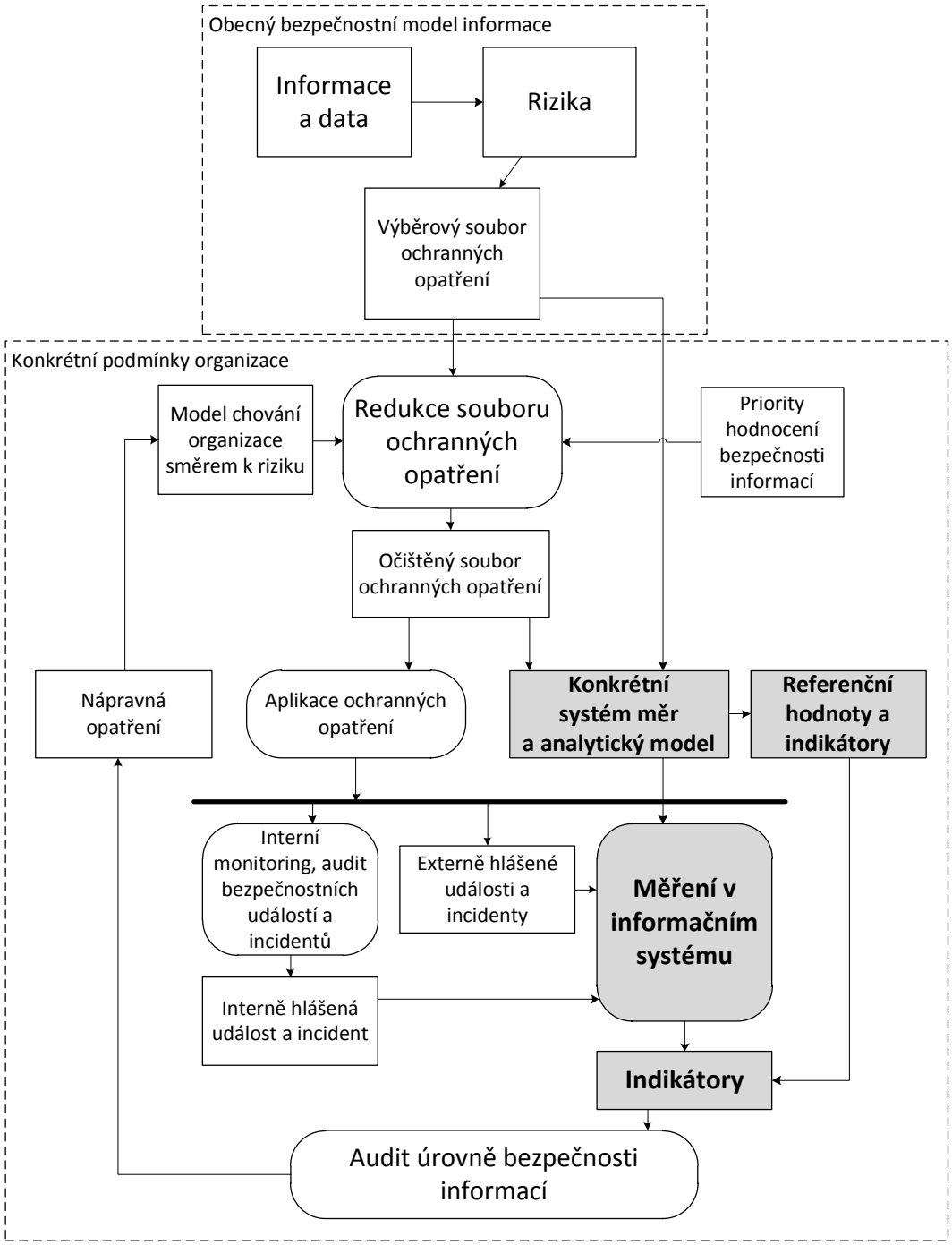
Postup vývoje (viz Schéma 9) obsahuje následující elementy:

- Zájmová **oblast rozšířeného bezpečnostního modelu** – hrozby, informace, ochrana, riziko;
- **Entity a relace** – soubor entit a relací rozšířeného bezpečnostního modelu (viz kap. 4. 5). Oblast měření také určuje soubor kontrolních opatření dle zvoleného standardu (např. ISO 27002:2009);
- **Základní soubor opatření podle zvoleného standardu** – soubor opatření pro aplikaci dle zvoleného standardu. V této práci je využit ISO 27002:2009;
- **Formální a kvalitativní kritéria míry** – zahrnuje kvalitativní, resp. kvantitativní zhodnocení akceptovatelnosti míry. V této práci je využito PRAGMATIC přístupu dle Brotby et al. (2013);
- **Formální definice míry a konstrukt GQM –** soubor parametrů a atributů specifikovaných podle teoretických předpokladů pro míru (viz kap. 4. 11, 10. 4);
- **Konstrukt míry podle šablony ISO 27004** – soubor parametrů a atributů specifikovaných v ISO 27004:2009 (viz kap. 10. 1).

5. 5 Model chování organizace s podporou měření

Z literárních zdrojů a provedeného průzkumu (kap. 4. 12) byl navržen zobecněný model chování organizace v České republice doplněný o aktivity měření úrovně bezpečnosti informací. metodou stanovení bezpečnostní pozice konkrétního informačního systému. Modifikace oproti zobecněnému modelu jsou zvýrazněny šedou barvou.

Schéma 10: Model chování organizace s podporou měření



Zdroj: vlastní zpracování

Účelem modifikace zobecněného modelu je zajistit v procesu pokrytí informační potřeby při provádění auditu úrovně bezpečnosti informací v informačním systému vytvořením konkrétního systému měr, referenčních hodnot a stanovením indikátorů.

Hlavní problémovou oblastí měření bezpečnosti informací je stanovení konkrétního na bezpečnostní charakteristiky informace zaměřeného systému měr, včetně stanovení referenčních (očekávaných) hodnot charakteristik objektů určených k měření. Stanovený systém měr má za cíl verifikovat úroveň účinku očištěného výběrového souboru ochranných opatření na relace bezpečnostního modelu a následnou validaci v provozu nasazených ochranných opatření.

Fáze měření v informačním systému lze realizovat některým z konstruktů norem identifikovaných v kap. 4. 11, tj. ISO 27004 (2009) a NIST SP800-55 (2008). Z komparace těchto konstruktů norem je zřejmé, že ISO 27004 poskytuje precizní metodický základ akademického typu pro vybudování systému měr. Současně je zřejmé, že ISO 27004 (2009, s. 2) vychází ze standardizovaných a formalizovaných normativních referencí ISO/IEC 9126 a ISO 15939.

NIST SP800-55 (2008) vychází z analýz standardizačního úřadu NIST a je přizpůsoben konkrétnímu prostředí amerických agentur. Hlavním problémem NIST standardu je chybějící definice postupu měření a to je důvodem, proč standard NIST SP800-55 nelze přímo pro měření použít.

Z pohledu volby aplikace uvedených norem pro měření byl autorem vybrán konstrukt měření dle ISO 27004, který je vhodný z důvodu své mezinárodní platnosti a vychází z normativních a vědeckých postupů. Lze také očekávat jeho další rozvoj.

5. 6 Návrh postupu pro hodnocení bezpečnosti informací

Hlavním cílem měření pozice informačního systému je možnost použít identifikované neúčinné relace modelu k jejich korekci pro další snižování rizika (posun směrem k vyšším hodnotám bezpečnosti informací, kap. 4. 3, Graf 1) a snižování míry redukce ochranných opatření v organizaci.

Návrh hodnocení bezpečnostní pozice je realizován pomocí komponent realizačního rámce (Tabulka 9):

Tabulka 9: Komponenty realizačního rámce

Komponenta	Reference	Diskutováno v kapitole
Konstrukt faktorů ovlivňujících bezpečnost informací v organizacích, konkrétně v podmínkách ČR	Vlastní zpracování	5. 1
Model chování organizace podporující měření	Vlastní zpracování	5. 5
Rozšířený konceptuální bezpečnostní model	Vlastní rozšířené zpracování	5. 3
Identifikace a verifikace měr pomocí GQM a formální konstrukt míry	Vlastní zpracování	5. 4 4. 11
Zhodnocení akceptovatelnosti míry	Brotby et al. (2013)	4. 11
Model měření a konstrukty měr ISO 27004	ISO 27004:2009	4. 11
Výběrová množina opatření MO_V	ISO 27002:2009	4. 11
Životní cyklus míry	Jaquith (2007, s. 244, 246)	4. 11

Zdroj: vlastní zpracování

Syntézou komponent realizačního rámce (Tabulka 9) je autorem definován dále popsaný rámcový metodický postup (Tabulka 10) pro hodnocení bezpečnostní pozice informačního systému, který byl ověřen v podmínkách konkrétních organizací v ČR.

Tabulka 10: Rámcový metodický postup měření

Krok postupu	Vstup	Aktivita	Výstup
1	Rozšířený konceptuální bezpečnostní model	Stanovení oblasti zájmu	Oblast zájmu
2	Oblast zájmu, vybrané entity a vazby	Stanovení cíle	Cíl (GOAL)
3	Cíl (GOAL)	Verifikace cíle na oblasti rozšířeného bezpečnostního modelu	Verifikovaný cíl (GOAL) nebo zamítnutý cíl
4	Verifikovaný cíl (GOAL)	Rozpad na otázky	Otázky (QUESTION)
5	Otázky (QUESTION)	Verifikace otázek na Rozšířeném bezpečnostním modelu	Verifikovaná otázka (QUESTION) nebo zamítnutá otázka
6	Verifikovaná otázka (QUESTION), sada opatření dle ISO 27002	Mapování opatření dle ISO 27002:2009 na Rozšířený bezpečnostní model	Mapa Entita, vztah na opatření dle ISO 27002:2009
7	Iterace krok 5 dokud není pokryt cíl		
8	Identifikace a definice míry (METRIC)	Stanovení iniciálního konstruktu míry a kvalitativních parametrů, měřicí nástroj	Iniciální konstrukt míry

9	Vývoj míry	Aktualizace iniciálního konstruktu a kvalitativních parametrů, měřicího nástroje, testování	Finální konstrukt míry a měřicí nástroj, analytický model a indikátory
10	Finální konstrukt míry	Zhodnocení akceptovatelnosti míry	Kvalitativní hodnota na škále výborná-nedostatečná, resp. PRAGMATIC skóre dle Brotby et al. (2013)
11	Finální konstrukt míry a měřicí nástroj, analytický model a indikátory	Konverze do konstruktu dle ISO 27004:2009	Finální konstrukt míry dle ISO 27004:2009
12	Finální konstrukt míry a měřicí nástroj	Nasazení míry a měření, sledování kvalitativních parametrů.	Průběžné výsledky měření
13	Průběžné výsledky měření	Vizualizace výsledků	Vizualizované výsledky měření
14	Vizualizované výsledky měření	Výpočet bezpečnostní pozice informačního systému, prezentace bezpečnostní pozice informačního systému	Hodnocení bezpečnosti informací, ohodnocení oblasti zájmu.
15	Hodnocení bezpečnosti informací, vliv ochranného opatření na kritické charakteristiky informace	Analýza výsledků, odvození hodnot indikátorů	Indikace, Odhad hodnot kritických charakteristik informace
16	Indikace, Odhad hodnot kritických charakteristik informace	Publikace výsledků a audit	Publikované výsledky a soubor nápravných opatření.

Zdroj: vlastní zpracování

Metodický postup je integrován do modelu chování organizace popsaného v kap. 5. 5.

5. 7 Prezentace bezpečnostní pozice informačního systému

Vyhodnocení bezpečnostní pozice systému využívá jeden z možných způsobů agregace výsledků měření a následného modelování podle rozšířeného bezpečnostního modelu. Využívá přitom skutečnosti, že cíle měření jsou validovány proti rozšířenému bezpečnostnímu modelu, měly by tedy přispívat v porozumění tomuto modelu a být do

tohoto modelu hypoteticky agregovatelné. Byl využit v případových studiích na vyvinutých mírách.

Navržený výpočet bezpečnostní pozice využívá k výpočtu techniku celkového ohodnocení vztahů v rozšířeném konceptuálním bezpečnostním modelu podle kap. 5. 3. Předpokládá se, že ohodnocení konkrétní kritické charakteristiky (C, I, A) informace *I* v čase *t* je funkcí účinnosti relací mezi entitami a současně neslabší množina relací identifikuje nejhorší pozici informačního systému v čase *t*.

Na model a jemu odpovídající instance entit je pohlíženo jako na neorientovaný ohodnocený graf, kde nejslabší posloupnost relací je možno vypočítat funkcí nejmenší kostry grafu (angl. minimal spanning tree). Výpočet je realizován aplikací Kruskalova algoritmu pro hledání nejmenší kostry v grafu.

Výsledná pozice systému informace v čase *t* je dána nejmenší kostrou, tj. vektorem vah hran

$$BP_{IS}\,(I,\ t) = (w(E_1, t), \ldots\ w(E_m, t))$$

kde:

m … počet hran zahrnutých v nejmenší kostře.

Aby bylo možno komparovat bezpečnostní pozice v různých časech $BP_{IS}(I,\ t_1)$ a $BP_{IS}(I, t_2)$, je třeba vzít v úvahu vliv redukce ochranných opatření, tj. vliv množiny $MO_R = MO_V \backslash MO_O$. Prezentace hodnoty $BP_{IS}\ (I, t)$ pak zahrnuje aktuální množinu MO_R. S ohledem na potenciální rozsáhlost této množiny je vhodné využít katalogů opatření uložených v technických databázových prostředcích, kde bude zafixován i konkrétní stav MO_R v čase *t*.

5. 7. 1 Konstrukce grafu

Při konstrukci grafu byla všem entitám přiřazena identifikační čísla 1-11 a model převeden do odpovídající incidenční matice (Tabulka 11). Vektor vah měr *W* je iniciálně nastaven na jednotkový vektor.

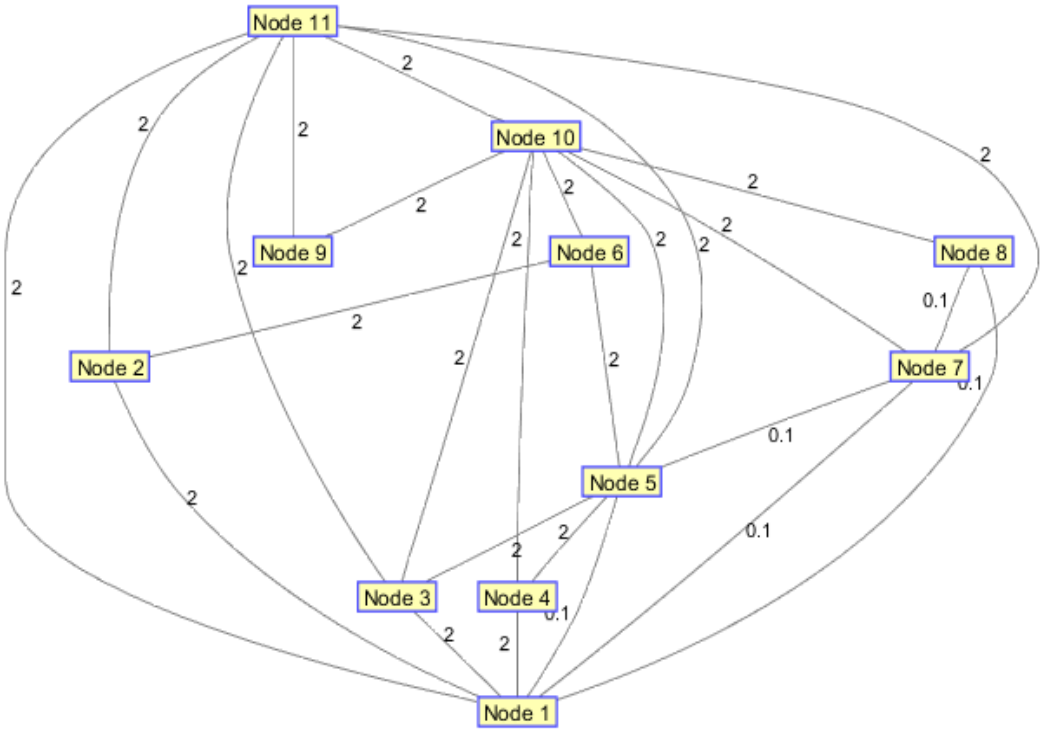
Tabulka 11: Incidenční matice Rozšířeného bezpečnostního modelu

		1	2	3	4	5	6	7	8	9	10	11
		Information	Value	Owner	Processor	Vulnerability	Impact	Threat	Threat agent	SecReq	Countermeasure	Risk
1	Information			cení	cení	vystavuje hrozbě		pro	cení			existuje pro
2	Value	má										
3	Owner											
4	Processor											
5	Vulnerability			zná	zná			těží z			má	
6	Impact		určuje			má					snižuje	
7	Threat								je podnětem		eliminuje	
8	Threat agent										odrazuje	
9	SecReq											indikuje
10	Countermeasure			vnucuje	realizuje			zvyšuje		jsou plněny		
11	Risk		zvyšuje	si přeje snížit		zvyšuje		zvyšuje			snižuje	

Zdroj: vlastní zpracování

Ideálně ohodnocená incidenční matice obsahuje plné ohodnocení všech hran. Váhy hran jsou negativní (maximální relativní ohodnocení = -1) a pozitivní (maximální ohodnocení = 1). Pro aplikaci výpočtu se zahrnutím negativně hodnocených vztahů byl rozsah <-1;1> vztahu superponován transformací T_W na interval (0; 2> (nulová hodnota byla vyloučena, neboť v Kruskalově algoritmu vyjadřuje neexistenci vazby). Při dalším vyhodnocováním jsou pak po výpočtu hodnoty přepočítány do původního intevalu odečtením hodnoty 1. Výchozí grafické znázornění uvádí Graf 2.

Graf 2: Grafické znázornění neohodnoceného grafu vazeb

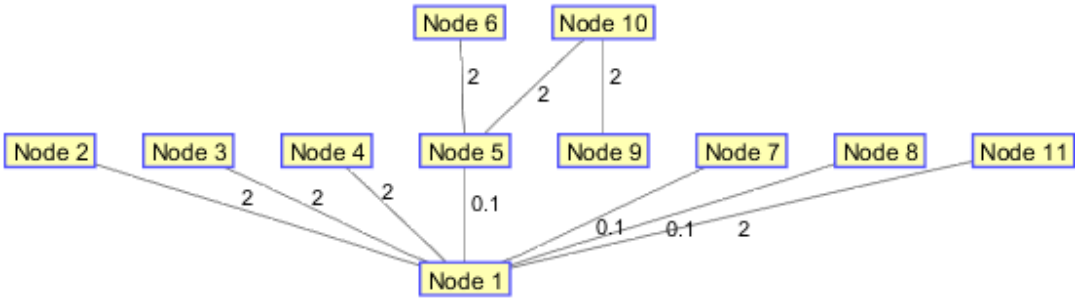


Zdroj: vlastní zpracování

Nad tímto grafem budou následně reálně ováhovány hrany grafu. Váhy u hran, které nejsou nijak hodnoceny, jsou nastaveny na neutrální hodnotu tak, aby nebyly upřednostňovány před ohodnocenými hranami, tj. u negativních vazeb pesimisticky na $w_{TW}(E_k)=0$, u pozitivních vazeb optimisticky na $w_{TW}(E_k)=2$.

Výpočet nejmenší kostry grafu nad ohodnoceným grafem Kruskalovým algoritmem následně vygeneruje strom, jehož hrany indikují jedno z nejmenších ohodnocení grafu – a tedy soubor nejslabších vazeb v grafu. Pro neohodnocený graf je výchozí stav následující:

Graf 3: Grafické znázornění stromu nejmenší kostry grafu



Zdroj: vlastní zpracování

5. 7. 2 Výpočet ohodnocení hrany grafu

Ohodnocení hrany E_k grafu využívá relativní škálu. Každý výsledek měření - míra μ_i (výstup z měřicí funkce pro odvození míry):

1. je relativizován na hodnotu $\mu_{Ri} \in \langle 0;1 \rangle$ s využitím rozsahů stanovených definovaným indikátorem přiřazeným míře, nebo přímo měřicí funkcí,
2. je určena váha odvozené míry $W(\mu_i) \in \langle 0;1 \rangle$,
3. je agregován do váhy hrany $w(E_k)$ s využitím váženého průměru

$$w(E_k) = \frac{\sum_{i=1}^{m} \mu_{Ri}.W(\mu_i)}{\sum_{i=1}^{m} W(\mu_i)}$$

kde:

m … počet odvozených měr tj. počet prvků množiny MO_O

Vztahem je zajištěno:

- vždy platí $w(E_k) \in \langle 0;1 \rangle$, a tím je zajištěn rozsah potřebný pro ohodnocení hrany grafu, u negativních vazeb je nutno váhu hrahy korigovat takto: $w(E_k) = -w(E_k)$
- již jedním měřením je možné ohodnotit hranu, tj. lze určit účinek relace v rozšířeném bezpečnostním modelu.

Uvedený postup agregace do analytického modelu je vhodný pro tvrdé míry postavených na kardinálních metrikách, které produkují reálná čísla, resp. celočíselné hodnoty a pravděpodobnosti. Pro měkké míry s nelineárním průběhem je nutné tuto míru transformovat vhodnou měřicí funkcí do kardinální stupnice.

5. 7. 3 Výpočet odhadu bezpečnostních charakteristik informace

Odhad hodnoty charakteristik C, I, A je dán souborem opatření příslušných ke každé hraně v nejmenší kostře a odhadem vlivu třídy T_O tohoto opatření na kritické charakteristiky informací (C, I, A) na základě odhadu podle Reference Monitoru v kap. 5. 2, sloupec „Výchozí odhad vlivu opatření“. Pokud jedno opatření patří do více tříd, započítává se pro každou třídu jako samostatné opatření.

$$C(I,t) = \frac{\sum_{i=1}^{o} V_{TO}\,(O_{i,}\,C).\mu_{Ri}}{\sum_{i=1}^{o} V_{TO}(O_i,C)}$$ (zdroj: vlastní zpracování)

$$I(I,t) = \frac{\sum_{i=1}^{o} V_{TO}\,(O_i,I).\mu_{Ri}}{\sum_{i=1}^{o} V_{TO}(O_i,I)}$$ (zdroj: vlastní zpracování)

$$A(I,t) = \frac{\sum_{i=1}^{o} V_{TO}\,(O_i,A).\mu_{Ri}}{\sum_{i=1}^{o} V_{TO}(O_i,A)}$$ (zdroj: vlastní zpracování)

kde:

o … počet opatření v očištěném souboru opatření MO_O

V_{TO} (O_i, x) … vliv konkrétní třídy opatření na kritickou charakteristiku v kontextu konkrétního opatření O_i

Zvolená funkce zajišťuje, že výstupy hodnot C, I, A jsou v rozsahu <0; 1>. Použité vztahy mají několik omezení. Předpokládají, že každé ochranné opatření je charakterizováno právě jednou odvozenou mírou. Pokud tomu tak není, což bude reálnější situace, je třeba každou míru dále agregovat do meta-opatření, na které lze použít odhad vlivu V_{TO}, resp. modifikovat vztah tak, aby odhad vlivu V_{TO} rozdělil mezi jednotlivé míry při zachování velikosti míry vlivu. V této práci je aplikován zjednodušený postup, kdy je míra s největší absolutní hodnotou přiřazena k opatření s největším vlivem. Tento přístup byl zvolen s ohledem na skutečnost, že případové studie probíhaly v časově stálém prostředí (množina opatření se neměnila) a od výpočtu se očekává „odhad“ kritických charakteristik.

S ohledem na počet odvozených měr a opatření je vhodné, aby výpočet probíhal časově odděleně od procesu měření dat. Doporučuje se realizovat tzv. kolektory údajů (technické sondy, monitory provozních žurnálů, resp. v případě fyzických opatření např. kamerovými záznamy).

6 VYHODNOCENÍ PRAKTICKÉ ČÁSTI

Následující kapitola shrnuje výsledky praktické části disertační práce v souladu s metodickým postupem uvedeným v kapitole 3. 2.

Výsledky průzkumu způsobů hodnocení bezpečnosti informací ve vybraných organizacích jsou uvedeny v kapitole 4. 12.

Výsledky kvantitativního výzkumu v organizacích v ČR sumarizující vlivné faktory na bezpečnost informací v těchto organizacích jsou shrnuty v kapitole 6. 1. 7.

Výsledky kvalitativního výzkumu technikou pohovorů zpřesňující oblasti pro hodnocení informačních systémů jsou shrnuty v kapitole 6. 2.

2 případové studie popisující aplikaci metodického postupu ve vybraných organizacích s vyhodnocením výstupů jsou uvedeny v kapitole 6. 3.

Závěry plynoucí z výstupů případových jsou uvedeny v kapitole 6. 3. 3.

6. 1 Kvantitativní výzkum

V rámci výzkumu bylo osloveno celkem N=785 organizací a od n=106 organizací se dotazník vrátil zcela vyplněný. Návratnost dotazníkového šetření je 13,5 %, což odpovídá teoretické návratnosti 10 až 25 % (Hendl, 2012) a je v souladu s doporučením Anderson (2009). Výsledky výzkumu ukazují, že v rámci zkoumaných organizací dochází ke zpracování informací (obchodní, účetní, zákaznické nebo jiné informace) výhradně počítačově (49,1 %), dále většinou počítačově (36,8 %). Lze konstatovat, že 85,9 % organizací zpracovává informace v současné době v počítačových informačních systémech. Pouze 2 organizace tento způsob zpracování nevyužívají vůbec. Jedná se o malé organizace v primárním sektoru.

Tabulka 12: Zpracovávání informací v informačních systémech

Forma informací	Absolutní četnost	Relativní četnost
Výhradně manuální	2	1,9
Většinou manuálních	11	10,4
Většinou počítačových	39	36,8
Výhradně počítačových	52	49,1
Nevím	2	1,9
Celkem	106	100,0

Zdroj: vlastní výzkum

Zástupci organizací uvedli, že jsou si vědomi, že zpracovávají hodnotné informace, jejichž ztráta nebo vyzrazení by znamenala škodu pro danou organizaci, případně pro jiné subjekty. Většina organizací, tj. 83,0 %, si tuto skutečnost uvědomuje. Pouze 2 zástupci organizací uvedli, že tyto hodnotné informace nezpracovávají a cíleně se jim vyhýbají. Dva zástupci si nebyli jisti, zda s hodnotnými informacemi (osobními údaji, údaji o klientech, či obchodními údaji či jiné) pracují.

Tabulka 13: Zpracovávání hodnotných informací

Forma informací	Absolutní četnost	Relativní četnost
Ano	88	83,0
Ne, cíleně se jim vyhýbáme,	2	1,9
Nemáme zjištěno, ale pravděpodobně ano.	13	12,3
Nemáme zjištěno, ale pravděpodobně ne.	1	0,9
Nevím	2	1,9
Celkem	**106**	**100,0**

Zdroj: vlastní výzkum

Na základě výše uvedeného byly z výzkumu vyřazeny organizace, které u druhé otázky uvedly, že se cíleně vyhýbají zpracování hodnotných informací či nevědí, zda tyto informace využívají (celkem 5 organizací). Ve všech 5 případech se jednalo o malé organizace do 20 zaměstnanců, přičemž 4 organizace byly z terciálního sektoru a 1 z primárního. Následně bylo ve výzkumu pracováno s výsledky u n=101 organizací (viz níže), kde většina organizací (87,1 %) pracuje s hodnotnými informacemi.

Tabulka 14: Zpracovávání hodnotných informací

Forma informací	Absolutní četnost	Relativní četnost
Ano	88	87,1
Pravděpodobně ano.	13	12,6
Celkem	**101**	**100,0**

Zdroj: vlastní výzkum

6. 1. 1 Vyhodnocení hypotézy 1

Hypotéza 1: V organizacích v ČR zpracovávajících hodnotné informace nejsou aplikovány postupy, standardy a normy řízení informační bezpečnosti na bázi mezinárodních ani harmonizovaných českých standardů. Hypotéza bude akceptována, pokud více než 75 % organizací neaplikuje postupy, standardy ani normy řízení informační bezpečnosti.

Na základě výsledků výzkumu bylo zjištěno, že více než 75 % organizací neaplikuje postupy, standardy ani normy řízení informační bezpečnosti na bázi standardů. Hypotézu lze akceptovat a lze shrnout, že v českých organizacích zpracovávajících hodnotné informace nejsou aplikovány postupy, standardy a normy řízení informační bezpečnosti na bázi mezinárodních ani harmonizovaných českých standardů.

V rámci výzkumu bylo zjišťováno, jaké systémy řízení informační bezpečnosti jsou využívány. Respondenti mohli zaznačit více odpovědí, tj. veškeré systémy řízení informační bezpečnosti, které využívají. Výsledky ukazují, že v 80,19 % organizacích jsou využívány zákonné normy a z 69,31 % vlastní interní směrnice a standardy. U 21,78 % organizací jsou využívány standardy ISO rodiny 27000.

Tabulka 15: Přehled využívání systémů řízení informační bezpečnosti

Systém řízení informační bezpečnosti	Absolutní četnost	Relativní četnost
Zákonné normy	81	80,19
Vlastní interní směrnice a standardy nezávislé na výše uvedených.	70	69,31
ISO rodiny 27000	22	21,78
ITIL	11	10,89
COBIT	7	6,93
ISO 13335 (ČSN ISO 13335)	5	4,95
Žádné	5	4,95
ISO 17799 (ČSN ISO 17799)	4	3,96
BS 7799 (ČSN BS 7799)	2	1,98
NIST SP-800	2	1,98
Jiné	0	0,00

Zdroj: vlastní zpracování

Systémy řízení informační bezpečnosti **ISO rodiny 27000** jsou nejčastěji využívány v terciálním sektoru z 90,9 %, v rámci primárního a sekundárního sektoru se jedná pouze o jednu organizaci, která tento systém využívá. V rámci velikosti organizace se jedná o využívání u velkých organizací a to ze 72,3 %. U malých a středních organizací se jedná o 22,7 % organizací, které je využívají.

Testováním závislostí mezi kvalitativními znaky bylo zjištěno, že existuje závislost mezi využíváním standardu rodiny ISO 27000 a velikostí organizace.

P-hodnota je nižší než hladina významnosti alfa (alfa = 0,05), a proto byla nulová hypotéza o neexistenci znaku zamítnuta a potvrzena hypotéza alternativní o existenci závislosti. P-hodnota = 0,000; test síly závislosti je Cramerovo V = 0,419 a jedná se o střední závislost. Rovněž byla potvrzena závislost mezi využíváním standardů rodiny ISO 27000 a sektorem ekonomiky. P-hodnota = 0,035; test síly závislosti je Cramerovo V = 0,210 a jedná se o slabou závislost.

Systém ISO 17799 (ČSN ISO 17799) je využíván shodně z 50 % v sekundárním i terciálním sektoru, jedná se však pouze o velké organizace (100,0 %).

Systém ISO 13335 (ČSN ISO 13335) se využívá ze 40,0 % v sekundárním sektoru a z 60,0 % v terciálním sektoru, jedná se však pouze o velké organizace (100,0 %). Malé a střední organizace ISO 13335 nepoužívají.

BS 7799 (ČSN BS 7799) je využívána ve 2 organizacích a ty působí v terciálním sektoru a jedná se o velké organizaci nad 250 zaměstnanců. NIST SP-800 je využíván rovněž u velkých organizací v terciálním sektoru (100,0 %).

COBIT je využíván u rovněž u velkých organizací v terciálním sektoru.

ITIL využívá celkem 11 organizací; 18,1 % (2 organizace) patří do sekundárního sektoru a jedná se o střední organizace, dále většina (81,9 %) organizací v terciálním sektoru a jedná se o velké organizace.

Zákonné normy jsou využívány u 70,3 % organizací v rámci terciálního sektoru a u 21,0 % u organizací v sekundárním sektoru a pouze u 8,7 % v primárním sektoru. Mezi sektorem organizace, ve kterém působí, a využíváním zákonných norem nebyla prokázána závislost, jelikož p-hodnota byla p = 0,186 a protože je vyšší než stanovená hladina významnosti alfa, nulovou hypotézu nelze zamítnout.

Podle zákonných norem primárně postupují velké organizace (39,5 %), dále 35,8 % malých organizací a 24,6 % středních organizací. Mezi velikostí organizace a využíváním zákonných norem nebyla prokázána závislost, jelikož p-hodnota byla p = 0,711 a protože je vyšší než stanovená hladina významnosti alfa, nulovou hypotézu nelze zamítnout.

Vlastní interní směrnice jsou využívány u malých, středních i velkých organizací (45,7 %). Mezi velikostí organizace a využíváním vlastních interních

směrnic a standardů nezávislých na výše uvedených byla prokázána statistická závislost. P-hodnota = 0,028; test síly závislosti je Cramerovo V = 0,219 a jedná se o slabší závislost. Mezi sektorem organizace, ve kterém působí, a využíváním interních směrnic však závislost prokázána nebyla, jelikož p-hodnota byla p = 0,728 a protože je vyšší než stanovená hladina významnosti alfa, nulovou hypotézu nelze zamítnout.

Dále bylo zjišťováno, které faktory mají dle respondentů hlavní vliv na dosažení maximální úrovně bezpečnosti informací v jejich organizaci. Respondenti mohli zaznačit více odpovědí. Mezi faktory, které mají v organizacích hlavní vliv na dosažení maximální úrovně bezpečnosti informací, byly respondenty nejčastěji zaznačeny faktory: „lidský faktor“ a „kvalita technických prostředků ochrany důvěrnosti, integrity a dostupnosti informací“.

Tabulka 16: Faktory s hlavním vlivem na úroveň bezpečnosti informací

Faktory	**Absolutní četnost**	**Relativní četnost [%]**
Lidský faktor	72	67,92
Kvalita technických prostředků ochrany důvěrnosti, integrity a dostupnosti informací	54	50,94
Existence identifikace rizik působících na konkrétní informační aktiva	45	42,45
Kvalita procesů řízení informační bezpečnosti a prosazování bezpečnostní politiky	40	37,74
Existence klasifikace informací	38	35,85
Monitoring osob, technických prostředků a informačních procesů	27	25,47
Měření bezpečnostních charakteristik informačního systému	18	16,98
Měření bezpečnostních charakteristik informací	11	10,38

Zdroj: vlastní výzkum

Faktor „identifikace rizik působících na konkrétní informační aktiva“ zaznačili nejčastěji zástupci středních organizací (52,3 %) působící v terciálním sektoru (77,3 %). Mezi velikostí organizace a identifikováním rizik v rámci organizace byla zjišťována statistická závislost. P-hodnota byla 0,098 a proto nelze nulovou hypotézu zamítnout. Rovněž nebyla potvrzena závislost mezi sektorem ekonomiky a identifikací rizik (p-hodnota = 0,424).

Faktor „prostředky ochrany důvěrnosti, integrity a dostupnosti informací“ zaznačili nejčastěji zástupci středních organizací (57,4 %) působící v terciálním sektoru (72,2 %), dále 22,2 % organizací v sekundárním sektoru. Mezi velikostí organizace a ochranou důvěrnosti byla zjišťována statistická závislost. P-hodnota byla 0,379 a tím pádem nelze nulovou hypotézu zamítnout. Rovněž nebyla potvrzena závislost mezi sektorem ekonomiky a identifikací rizik (p-hodnota = 0,799).

Faktor „klasifikace informací“ zaznačili nejčastěji zástupci středních organizací (47,4 %) působící v terciálním sektoru (65,8 %), dále 26,3 % organizací v sekundárním sektoru. Mezi velikostí organizace a klasifikací informací byla zjišťována statistická závislost. P-hodnota byla 0,025 a tedy lze nulovou hypotézu zamítnout. P-hodnota = 0,025; test síly závislosti je Cramerovo V = 0,224 a jedná se o slabší závislost. Mezi sektorem ekonomiky a důrazem na klasifikaci informací nebyla závislost potvrzena (p-hodnota = 0,131).

Celkem 75,0 % zástupců organizací označilo „lidský faktor“ za faktor, který má v organizacích zásadní vliv na dosažení maximální úrovně bezpečnosti informací. Dále tento faktor označilo 12,5 % zástupců z primárního i sekundárního sektoru. Závislost mezi klasifikací informací a sektorem ekonomiky prokázána nebyla (p-hodnota = 0,535). Při rozlišení organizací dle velikosti je lidský faktor vlivnější v malých a středních organizacích (63,9 %). Nulová hypotéza hovořící o neexistenci závislosti mezi velikostí organizace a uvedení lidského faktoru za vlivný faktor dosažení maximální úrovně bezpečnosti zamítnuta nebyla, jelikož p-hodnota = 0,416.

Faktor „kvality procesů“ uvádělo 77,5 % organizací, které působí v terciálním sektoru a celkem 22,5 % organizací v sekundárním sektoru. V rámci primárního sektoru nezaznačil tento faktor žádný zástupce organizace. Nulová hypotéza zamítnuta nebyla, jelikož p-hodnota = 0,436 a je vyšší než hladina významnosti alfa (0,05). V případě velikosti organizace tuto odpověď uvedla většina velkých organizací (72,5 %). Rovněž byla zjištěna závislost mezi velikostí organizace a uvedení faktoru kvality procesů. P-hodnota = 0,000; Cramerovo V = 0,564, což je silná závislost.

„Monitoring osob, technických prostředků a informačních procesů“ byl uveden u 77,8 % organizací v terciálním sektoru, u 18,5 % organizací v sekundárním sektoru a jen u 1 organizace v rámci primárního sektoru (3,7 %) a jednalo se převážně o velké

organizace (59,3 %). Mezi faktorem monitoringu osob a velikostí organizace byla zjištěna statistická závislost. P-hodnota = 0,010; Cramerovo V = 0,256 a to je slabší závislost. U sektoru ekonomiky závislost prokázána nebyla (p-hodnota = 0,536).

„Měření bezpečnostních charakteristik informačního systému“ uváděli nejčastěji zástupci organizací působící v terciálním sektoru (83,3 %) a ostatní zástupci organizací v sekundárním sektoru. V rámci primárního sektoru tento faktor není považován za vlivný. Jedná se o většinu velkých organizací (77,8 %). Mezi velikostí organizace a měřením bezpečnostních charakteristik informačního systému existuje statistická závislost a nulová hypotéza o nezávislosti byla proto zamítnuta. P-hodnota = 0,000; Cramerovo V = 0,375 a jedná se o střední závislost.

„Měření bezpečnostních charakteristik informací“ uvedlo jako důležitý faktor celkem 90,9 % organizací v terciálním sektoru a pouze 1 organizace v sekundárním sektoru. Z 81,8 % se jedná o velké organizace, které tuto odpověď prostřednictvím svých zástupců uvedlo. Statistická závislost mezi velikostí a sektorem ekonomiky a zkoumaným faktorem zde nebyla prokázána.

6. 1. 2 Vyhodnocení hypotézy 2

Hypotéza 2: Organizace v ČR zpracovávající hodnotné informace nestanovují priority cílů (nehodnotí cíle shodně) v oblasti bezpečnosti informací. Hypotéza bude akceptována, pokud méně než 50 % organizací stanoví důležitost bezpečnostních cílů odlišně. Stanovení priorit = ohodnocení důležitosti organizačních cílů v konkrétní organizaci při dosahování bezpečnosti informací (1= zcela nedůležitá, 5= velmi důležitá, je možné přiřadit stejnou důležitost). V případě, že organizace stanoví u všech cílů stejnou důležitost (např. u všech hodnotu 5= velmi důležitá), jedná se o nestanovení priorit. V případě, že alespoň u jednoho cíle stanoví organizace důležitost jinou než u ostatních, jedná se o stanovení priorit cílů.

Na základě výsledků bylo zjištěno, že organizace v České republice, které zpracovávají hodnotné informace, stanovují priority cílů v oblasti bezpečnosti informací. Bylo zjištěno, že oblast splnění legislativních cílů je pro organizace v ČR nejdůležitější a dále pak splnění personálních cílů. To je v souladu s výsledkem hypotézy č. 4.

V rámci vyhodnocení této otázky mohli respondenti zaznačit více odpovědí. Průměrná známka v rámci ekonomických cílů byla 3,75. U oblasti personálních cílů byla průměrná známka 3,79. U technických cílů 3,54 a u legislativní 3,94, což je nejvyšší průměrné číslo. Lze tedy konstatovat, že legislativní cíle staví zkoumané organizace nejvýše v hierarchii cílů a nejméně pak technické. Podrobné výsledky jsou uvedeny v tabulce níže.

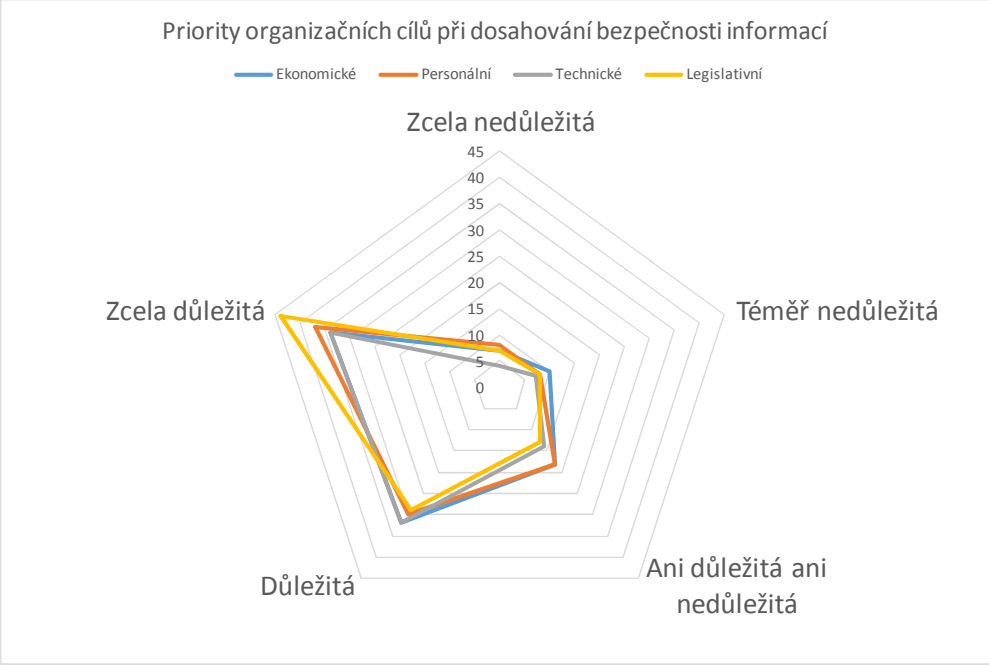
Tabulka 17: Důležitost organizačních cílů ve vztahu k bezpečnosti informací

Organizační cíl	**Zcela nedůležitá**	**Téměř nedůležitá**	**Ani důležitá ani nedůležitá**	**Důležitá**	**Zcela důležitá**	**Suma**
Legislativní	7	8	13	29	44	101
Personální	8	8	18	30	37	101
Ekonomické	7	10	18	32	34	101
Technické	4	7	14	32	34	101
Suma	**26**	**33**	**63**	**123**	**149**	**X**

Zdroj: vlastní výzkum

Pro snazší orientaci jsou výsledky zobrazeny v pavučinovém grafu, který srovnává zkoumané oblasti v závislosti na absolutních četnostech odpovědí.

Graf 4: Identifikace důležitosti bezpečnosti informací v rámci organizačních cílů



Zdroj: vlastní výzkum

6. 1. 3 Vyhodnocení hypotézy 3

Hypotéza 3: Kvantitativní přístup k hodnocení bezpečnosti informací v organizacích v ČR zpracovávajících hodnotné informace není aplikován. Hypotéza bude akceptována, pokud více než 80 % organizací neaplikuje měření, resp. kvantitativní hodnocení bezpečnosti informací v informačním systému.

Před zjišťováním přístupu k hodnocení bezpečnosti informací kvantitativním přístupem byl zjišťován postoj organizací k hodnocení bezpečnosti informací obecně. Následně byl výzkum zaměřen na kvantitativní metody hodnocení.

Celkem 62 organizací (61,4 %) uvedlo, že hodnotí bezpečnost informací a 38,6 % (39 organizací) tuto oblast nehodnotí. Nejvíce hodnotí bezpečnost informací organizace v terciálním sektoru (ze 77,4 %), dále pak ze sekundárního (19,4 %) a následně až z primárního (3,2 %). Nejvíce hodnotí bezpečnost informací velké organizace nad 250 zaměstnanců (54,8 %). Mezi velikostí organizace a hodnocením bezpečnosti informací existuje statistická závislost. P-hodnota = 0,000; Cramerovo V = 0,420 a jedná se o střední závislost. U sektoru ekonomiky závislost prokázána nebyla, jelikož p-hodnota = 0,235.

Vzhledem k tomu, že téměř 40 % zkoumaných organizací bezpečnost informací nehodnotí, byly zjišťovány důvody, proč tomu tak je. Respondenti mohli zaznačit více odpovědí. Za hlavní důvod nehodnocení bezpečnosti informací uváděli, že předpokládají, že informační systém, který informace zpracovává, je bezpečný. Podrobnější údaje uvádí Tabulka 18.

Tabulka 18: Důvody nehodnocení bezpečnosti informací

Důvody	Absolutní četnost	Relativní četnost
Předpokládáme, že informační systém je bezpečný.	29	28,71
Neexistují postupy pro hodnocení, resp. nevíme co hodnotit.	12	11,88
Nepovažujeme to za důležité	10	9,90
Postupy pro hodnocení jsou finančně či jinak náročné.	3	2,97

Zdroj: vlastní výzkum

Důvod, že hodnocení bezpečnosti informací nepovažují za důležité, uvedly 2 organizace z primárního sektoru a 8 z terciálního. Všechny organizace patří do

kategorie malé a střední. Předpoklad bezpečnosti zpracovávajícího informačního systému uvedlo celkem 19 organizací (65,5 %) z terciálního sektoru, 4 ze sekundárního (13,8 %) a 6 (20,7 %) z primárního. Z 83,5 % se jednalo o malé a střední organizace, které toto uvedly. Byla prokázána statistická závislost mezi odpovědí, že předpokládají, že informační systém je bezpečný a velikostí organizace. P-hodnota = 0,005; Cramerovo V = 0,279 a jedná se o slabší závislost. U sektoru závislost prokázána nebyla, jelikož p-hodnota = 0,264.

Důvod, že neexistují postupy pro hodnocení, respektive organizace nevědí, co hodnotit, uvedlo celkem 12 organizací, z toho 58,3 % z terciálního sektoru, 25,0 % z primárního sektoru a 26,7 % ze sekundárního sektoru. Jednalo se v 83,3 % případů o malé a střední organizace.

Poslední možnost, tj. že postupy pro hodnocení jsou pro organizaci drahé, uvedly celkem 3 malé organizace, 2 byly z terciálního sektoru a jedna z primárního.

Vzhledem ke skutečnosti, že 61,4 % zkoumaných organizací bezpečnost informací hodnotí, byl zjišťován cíl hodnocení, tedy důvod, který organizace vede k této činnosti. Nejčastěji je to důvod „včasné identifikace vznikajících problémů a slabin“ (43,56 %) a dále „zlepšování procesů informační bezpečnosti“ (38,61). Podrobnější výsledky uvádí Tabulka 19.

Tabulka 19: Cíl hodnocení bezpečnosti informací

Cíl hodnocení	Absolutní četnost	Relativní četnost
Identifikace vznikajících problémů a slabin.	44	43,56
Zlepšování procesů informační bezpečnosti.	39	38,61
Pokrytí legislativních požadavků.	38	37,62
Potvrzení účinnosti nastavených protiopatření.	34	33,66
Porozumění bezpečnostním rizikům.	31	30,69

Zdroj: vlastní výzkum

Za cíl „porozumění bezpečnostním rizikům“ si kladou hlavně organizace v terciálním sektoru (90,3 %) a dále v sekundárním sektoru (9,7 %). V primárním sektoru není tento cíl důležitý. Jedná se o 58,0 % velkých organizací, které si tento cíl stanovují. Mezi velikostí organizace a stanovením tohoto cíle existuje statistická závislost. P-hodnota = 0,008; Cramerovo V= 0,266 a jedná se o slabší závislost.

Cíl „identifikace vznikajících problémů a slabin“ si stanovuje celkem 81,8 % organizací v terciálním sektoru, 15,9 % organizací v sekundárním sektoru a pouze

1 organizace v sektoru primárním. Závislost mezi stanovením tohoto cíle a sektorem ekonomiky prokázána nebyla (p-hodnota = 0,088). Tento cíl si ze 75,0 % stanovují velké organizace. Byla prokázána závislost mezi velikostí organizace a tímto cílem. P-hodnota = 0,000; Cramerovo V= 0,534 a jedná se o střední závislost.

„Potvrzení účinnosti nastavených protiopatření“ uvedlo jako cíl 82,4 % organizací v terciálním sektoru, 14,7 % organizací v sekundárním sektoru a pouze 1 organizace v sektoru primárním. Jedná se u 58,8 % o velké organizace a mezi velikostí organizace a stanovením tohoto cíle byla zjištěna závislost. P-hodnota = 0,003; Cramerovo V=0,296 a jedná se o slabší až střední závislost. Závislost mezi stanovením tohoto cíle a sektorem ekonomiky prokázána nebyla (p-hodnota = 0,142).

„Zlepšování procesů informační bezpečnosti“ si jako cíl stanovuje celkem 76,9 % organizací působící v terciálním sektoru, 20,5 % organizací v sekundárním a 1 v primárním sektoru. Z 63,1 % se jedná o velké organizace nad 250 zaměstnanců a mezi velikostí organizace a stanovením tohoto cíle byla zjištěna závislost. P-hodnota = 0,000; Cramerovo V=0,415 a jedná se o střední závislost. Závislost mezi stanovením tohoto cíle a sektorem ekonomiky prokázána nebyla (p-hodnota = 0,510).

Cíl „pokrytí legislativních požadavků“ si stanovuje nadpoloviční většina v rámci terciálního sektoru (78,9 %), dále 15,8 % ze sekundárního sektoru a 2 organizace z primárního sektoru. Z 68,4 % se jedná o velké organizace nad 250 zaměstnanců a mezi velikostí organizace a stanovením tohoto cíle byla zjištěna závislost. P-hodnota = 0,000; Cramerovo V=0,475 a jedná se o střední závislost. Závislost mezi stanovením tohoto cíle a sektorem ekonomiky prokázána nebyla (p-hodnota = 0,316).

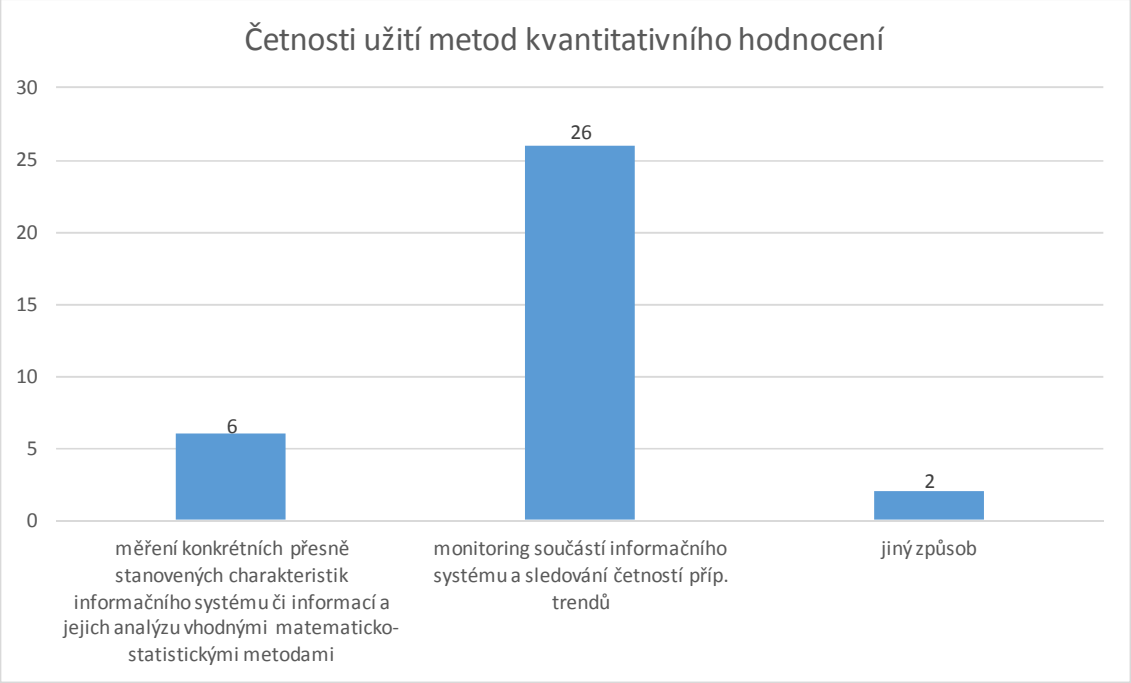
V oblasti kvantitativního přístupu k hodnocení bezpečnosti informací výsledky ukázaly, že celkem 59,4 % organizací neaplikuje měření, resp. kvantitativní hodnocení bezpečnosti informací v informačním systému. Dalších 6,9 % respondentů uvedlo, že nevědí, zda toto měření provádí. Lze tedy konstatovat, že z největší pravděpodobností měření taktéž neprovádí. Jednalo by se proto celkem o 66,3 % organizací.

Celkem 34 organizací (33,7 %) uvedlo, že měření bezpečnosti informací provádí. Jedná se o organizace převážně v terciálním sektoru (73,5 %) a dále v sekundárním sektoru (23,5 %). V primárním sektoru aplikuje měření pouze jedna organizace z 10 oslovených.

V případě zohlednění velikosti organizace lze říci, že měření bezpečnosti informací provádí hlavně organizace velké (58,8 %). Malé organizace měření bezpečnosti neprovádějí nebo si nejsou jisti, zda tuto aktivitu realizují.

Pokud je měření bezpečnosti informací realizováno, jedná se ze 76,5 % o monitoring součástí informačního systému a sledování četností případně trendů u 17,6 % organizací jde o měření konkrétních přesně stanovených charakteristik informačního systému a jejich analýzu vhodnými matematicko-statistickými metodami. Celkem ve 2 organizacích bylo uvedeno, že se využívají jiný způsob, neuvedli však který.

Graf 5: Využívané způsoby kvantitativního hodnocení bezpečnosti informací



Zdroj: vlastní výzkum

Celkem 76,9 % organizací z terciálního sektoru, které měření bezpečnosti informací realizují, aplikují monitoring a ostatní měření konkrétních přesně stanovených charakteristik. V rámci sekundárního sektoru je aplikován monitoring (23,1 %). Jedna organizace, která se měřením bezpečnosti informací zabývá z primárního sektoru, realizuje měření konkrétních charakteristik informací. Z hlediska zohlednění velikosti organizace lze dle výsledků říci, že monitoringem se zabývá 57,7 % velkých organizací, ostatní měřením konkrétních přesně stanovených charakteristik.

Lze tedy konstatovat, že monitoringem se nejčastěji zabývá velká organizace v rámci terciálního sektoru.

6. 1. 4 Vyhodnocení hypotézy 4

Hypotéza 4: Předpokládá se, že vlivné faktory na dosažení maximální úrovně bezpečnosti informací považuje za důležité většina organizací. Hypotéza bude akceptována, pokud každý faktor bude uveden více než u 50 % organizací.

Výsledky ukázaly, že většina organizací považuje za nejvlivnější faktor dosažení maximální úrovně bezpečnosti informací lidský faktor (67,92 % organizací) a faktor kvality technických prostředků ochrany důvěrnosti, integrity a dostupnosti informací (50,94 % organizací). Ostatní faktory se pohybovaly v relativní četnosti 10,38 % (11 organizací ze 101) až 42,45 % (45 odpovědí). Střední hodnota odpovědí je 35,97 %. Na základě stanovené hypotézy a zjištěných výsledků nelze proto jednoznačně uvést, že všechny identifikované faktory jsou manažery pokládány za důležité, lze to však jednoznačně uvést u lidského faktoru a kvality technických prostředků ochrany důvěrnosti, integrity a dostupnosti informací.

Pro získání podrobnějších výsledků byly aplikovány nástroje vícerozměrné statistiky a to faktorová a shluková analýza.

6. 1. 5 Výsledky faktorové analýzy

Metodou Varimax byly nalezeny dva faktory. Rozptyl u faktoru 1 byl vyšší než u faktoru 2 (přes 36 %), proto tento rozptyl lze považovat za největší. V tabulce 2 jsou prezentovány výsledky rozptylů významných faktorů vysvětlující proměnné. Program IBM SPSS Statistics Desktop 21 pomocí metody Varimax identifikoval celkem 2 faktory, jejichž vlastní číslo (rozptyl) je vyšší než 1 (Kaiser-Guttmanovo pravidlo). Celkově tyto dvě identifikované proměnné (přes 50 %) vysvětlují celkové chování vzorku či možností výsledných vlastností. Cílem faktorové analýzy je charakterizovat nově vzniklé proměnné na základě závislostí (hodnotě korelačního koeficientu) s původními proměnnými.

Tabulka 20: Výpočet rozptylu významných faktorů

Faktor	Rozptyl	% rozptylu	Kumulativní % rozptylu
1	2,902	36,279	36,279
2	1,131	14,135	50,414

Zdroj: Vlastní výzkum

První faktor poukazuje na důležitost bezpečnostních procesů na organizační úrovni a jak sledovaná organizace klade důraz na oblast bezpečnosti informací (viz tabulka 3). Faktor je nejvíce tvořen měřením bezpečnostních charakteristik informací (0,788), měřením bezpečnostních charakteristik informačního systému (0,738) a monitoringem osob (0,737), prostředky ochrany důvěrnosti a informačními procesy. Lze jej tedy souhrnně pojmenovat „elementy bezpečnostních procesů“. Korelační koeficienty se pohybují v rozmezí od 0,397 do 0,788, což představuje střední a silnou závislost (u většiny koeficientů).

Druhý identifikovaný faktor zahrnuje dvě proměnné na obecné úrovni, proto jej lze nazvat „bezpečnostně kritické prvky“. Nejsilnějším faktorem z hlediska bezpečnostně kritických prvků je lidský faktor (0,825). Oba koeficienty (lidský faktor i klasifikace informací) představují silnou závislost (0,637 a silnější).

Tabulka 21: Výpočty faktorové analýzy

Proměnná	Faktor 1	Faktor 2
Identifikace rizik působících na konkrétní informační aktiva	**0,397**	0,375
Prostředky ochrany důvěrnosti, integrity a dostupnosti informací	**0,559**	0,133
Klasifikace informací	0,299	**0,637**
Lidský faktor	-0,174	**0,825**
Kvalita procesů řízení informační bezpečnosti a prosazování bezpečnostní politiky	**0,663**	-0,018
Monitoring osob, technických prostředků a informačních procesů	**0,737**	0,091
Měření bezpečnostních charakteristik informačního systému	**0,738**	0,042
Měření bezpečnostních charakteristik informací	**0,788**	0,200
Celkové % rozptylu	**36,279**	**14,135**
Název faktoru	Bezpečnostní procesy	Bezpečnostně kritické prvky

Zdroj: Vlastní výzkum

Lze shrnout, že hlavními faktory ovlivňujícími bezpečnost informací jsou *bezpečnostní procesy* v organizaci, z nichž velkou část tvoří monitoring a měření a kvalita procesů, a faktor *bezpečnostně kritické prvky* informačního systému tvořené především lidským faktorem a následně bezpečnostní klasifikací informací.

Dále byla zjišťována závislost faktorů na odvětví. Metodou Varimax byly nalezeny tři faktory. Rozptyl u faktoru 1 byl vyšší než u faktoru 2 a 3 (přes 32 %), proto tento rozptyl lze považovat za největší. Tabulka 22 prezentuje výsledky rozptylů významných faktorů vysvětlující proměnné.

Tabulka 22: Výpočet rozptylu významných faktorů

Faktor	**Rozptyl**	**% rozptylu**	**Kumulativní % rozptylu**
1	2,912	32,353	36,353
2	1,181	13,126	45,478
3	1,100	12,219	57,697

Zdroj: vlastní výzkum

Při sestavení faktorové analýzy (viz Tabulka 23) se vycházelo z předpokladu, že proměnná sektor ekonomiky (sloučený primární a sekundární sektor) je považována za němou proměnnou (kladná nebo záporná závislost byla dále vysvětlena ve smyslu jejího výsledného působení tak, jak byly kódovány odpovědi respondentů vstupující do analýzy).

Na základě statistických výpočtů lze proto konstatovat, že první faktor a nejsilnější faktor je tvořen *bezpečnostními procesy*, korelační koeficient se pohybuje mezi 0,435 u identifikace rizik a 0,812 u měření bezpečnostních charakteristik informací. Z výsledků lze usuzovat, že se jedná o terciální sektor. Lze shrnout, že identifikace faktorů a přizpůsobení organizačních podmínek primárně v oblasti měření bezpečnostních charakteristik informačního systému a měření bezpečnostních charakteristik informací, u kterých byl prokázán nejvyšší korelační koeficient, je v terciálním sektoru vnímána jako nejdůležitější.

Tabulka 23: Výsledky faktorové analýzy s němou proměnnou

Proměnná	Faktor 1	Faktor 2	Faktor 3
Identifikace rizik působících na konkrétní informační aktiva	**0,435**	**0,318**	0,064
Prostředky ochrany důvěrnosti, integrity a dostupnosti informací	**0,546**	0,031	**0,400**
Klasifikace informací	0,323	**0,488**	**0,545**
Lidský faktor	-0,084	**0,889**	-0,088
Kvalita procesů řízení informační bezpečnosti a prosazování bezpečnostní politiky	**0,653**	-0,132	0,166
Monitoring osob, technických prostředků a informačních procesů	**0,740**	0,041	0,000
Měření bezpečnostních charakteristik informačního systému	**0,745**	0,045	-0,164
Měření bezpečnostních charakteristik informací	**0,812**	0,181	-0,117
Sektor ekonomiky (primární a sekundární)	0,189	0,092	-0,801
Celkové % rozptylu	**32,353**	**13,126**	**12,219**
Název faktoru	Bezpečnostní procesy	Bezpečnostně kritické prvky	Ochrana citlivých dat

Zdroj: vlastní zpracování

U faktoru 1 vychází také velmi silná závislost u monitoringu osob, technických prostředků a informačních procesů (0,740, silná přímá závislost). První faktor lze proto nazvat „bezpečnostní procesy“. Druhý faktor, který se zabývá bezpečnostně kritickými prvky (korelační koeficient 0,488 a 0,889, což je silná závislost) a reflektuje výsledky v tabulce. Třetí faktor uvádí, že bezpečnost informací je ovlivněna klasifikací informací a prostředky ochrany důvěrnosti, integrity a dostupnosti informací.

6. 1. 6 Výsledky shlukové analýzy

Pro zjištění blízkosti odpovědí u jednotlivých faktorů byla použita rovněž shluková analýza. Na základě výsledků shlukové analýzy byla nalezena struktura mezi objekty. Vysvětlení, proč tato struktura existuje, je dále okomentována autorem na základě praktických zkušeností a výsledků kvalitativního výzkumu formou rozhovorů. Pro zpracování výsledků byly využity shluky jednotek, které mají k sobě nejblíže (tj. metoda nejbližšího souseda dle významové shody), konkrétně byla využita euklidovská vzdálenost pomocí Wardovy metody, jež je založena na souhrnné změně

vnitroskupinové variability sledovaných proměnných pro vytvoření nového shluku, což je v souhladu s Pacákovou, (2011), Hendlem (2012). Tabulka 24 zobrazuje kombinaci jednotlivých shluků a identifikuje sousedy.

Tabulka 24: Výpočet shlukové analýzy

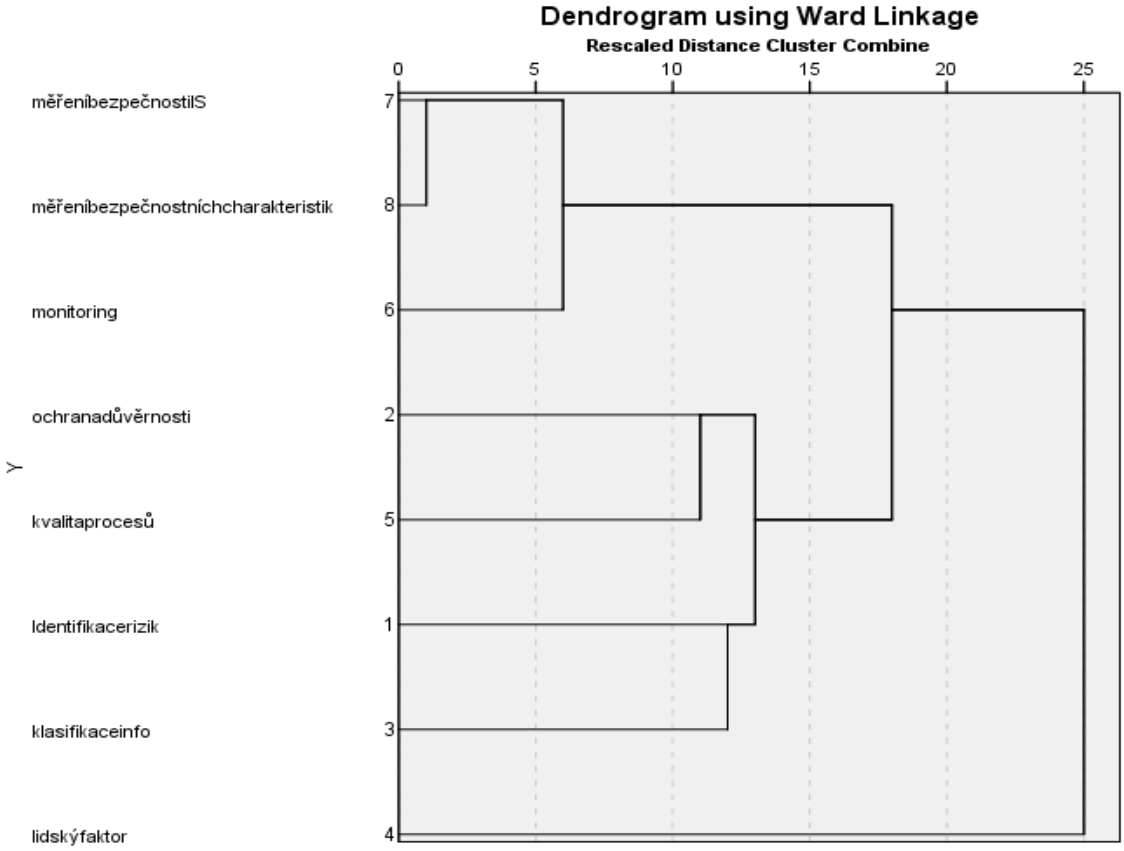
Proměnná	**Legenda**	**Kombinace shluků**		**Koeficient**
		Shluk 1	**Shluk 2**	
Identifikace rizik působících na konkrétní informační aktiva	1	**7**	**8**	4,500
Prostředky ochrany důvěrnosti, integrity a dostupnosti informací	2	**6**	**7**	16,000
Klasifikace informací	3	**2**	**5**	34,000
Lidský faktor	4	**1**	**3**	53,500
Kvalita procesů řízení informační bezpečnosti a prosazování bezpečnostní politiky	5	**1**	**2**	75,250
Monitoring osob, technických prostředků a informačních procesů	6	**1**	**6**	103,429
Měření bezpečnostních charakteristik informačního systému	7	**1**	**4**	141,625
Měření bezpečnostních charakteristik informací	8	x	X	X

Zdroj: vlastní zpracování

Pro grafické znázornění výsledků shluků byl využit dendrogram, který zobrazuje nejbližší proměnné respondentů na výzkumné otázky v dotazníkovém šetření.

Soubor proměnných se na základě zobrazení pomocí dendrogramu rozpadl na 4 základní shluky (podskupiny, hranice vzdálenosti spoje je 25), celkem jich bylo nalezeno 7. Dendrogram získaný na základě euklidovské vzdálenosti metodou úplného spojení zobrazuje, že první shluk je tvořen vnitřními determinanty popisujícími měření bezpečnosti informací a měření bezpečnostních charakteristik informací. Daná kombinace determinantů vypovídá o specifičnosti používaných metod k měření v různých odvětvích a rozdílný přístup k této oblasti z řad vedení organizací.

Graf 6: Dendrogram faktorů



Zdroj: vlastní výzkum

Druhý shluk je tvořen monitoringem a měřením bezpečnosti informací. Na základě uvedeného lze říci, že když se organizace měřením bezpečnosti zabývá, jedná se většinou o techniku monitoringu prvků informačních systémů a sledování četností případně trendů, které organizaci mohou ohrozit. Ve třetím shluku se objevují prostředky ochrany důvěrnosti, integrity a dostupnosti informací a kvalita procesů řízení informační bezpečnosti a prosazování bezpečnostní politiky. Čtvrtý shluk je tvořen „identifikací rizik působících na konkrétní informační aktiva“ a „klasifikací informací“.

Z hlediska výzkumu je nejdůležitější shluk č. 1, který zahrnuje blízké vzdálenosti mezi odpověďmi na otázky týkajících se měření bezpečnosti informací a měření jejich bezpečnostních charakteristik. To vše poukazuje, že v případě, že se organizace zabývá měřením bezpečnosti informací, je to realizováno s cílem neohrozit organizaci, eliminovat co nejvíce hrozby a podporovat proaktivní chování organizace.

Z dalších menších shluků lze např. identifikovat vztah determinantů „prostředků ochrany důvěrnosti, integrity a dostupnosti informací“ a „kvality procesů řízení informační bezpečnosti a prosazování bezpečnostní politiky“. Rovněž pak existuje vztah mezi identifikací rizik působících na konkrétní informační aktiva a monitoringem osob, technických prostředků a informačních procesů.

Struktura respondentů

Vzhledem k teoretickým předpokladům a zpracování výzkumu tak, aby reflektoval složení organizací dle sektoru v rámci ČR, bylo osloveno celkem 73,3 % organizací v terciálním sektoru, 16,8 % organizací v sekundárním sektoru a 9,9 % organizací v primárním sektoru. Rozložení odpovídá složení dle ČSÚ (2012).

Tabulka 25: Struktura organizací dle sektoru ekonomiky

Sektor	Absolutní četnost	Relativní četnost
Primární	10	9,9
Sekundární	17	16,8
Terciální	74	73,3
Celkem	101	100,0

Zdroj: vlastní výzkum

Složení organizací podle velikosti bylo přibližně proporcionální, tedy 37,6 % malých organizací, 23,8 % středních organizací a 38,6 % velkých organizací.

Tabulka 26: Struktura organizací dle velikosti organizace

Sektor	Absolutní četnost	Relativní četnost
Malé	38	37,6
Střední	24	23,8
Velké	39	38,6
Celkem	101	100,0

Zdroj: vlastní výzkum

S ohledem na většinový podíl se jedná ze 77,2 % o české organizace a z 22,8 % o zahraniční organizace (mají více než 50% zahraniční vlastnický podíl). Jedná se většinou o strategické aliance a nadnárodní organizace s pobočkami po celém světě.

Tyto organizace svým dceřiným společnostem udávají organizační kulturu a politiku a lze očekávat ovlivnění i zkoumaného chování.

Tabulka 27: Struktura organizací dle majoritního vlastnického podílu

Sektor	Absolutní četnost	Relativní četnost
České organizace	78	77,2
Zahraniční organizace	23	22,8
Celkem	101	100,0

Zdroj: vlastní výzkum

Zkoumané společnosti nejvíce využívají outsourcing služeb (mohli zaznačit více odpovědí) v oblasti IT pro internetové připojení (84,16 %) a následně pro finanční či účetní systém (46,53 %) a nejméně pro bezpečnostní monitoring (17,82 %). Z jiných možností byl uveden outsourcing nemocničního informačního systému, poradenské právní služby, záložní datové centrum či uvedení, že outsourcing nevyužívají.

Tabulka 28: Využívání outsourcingu na jednotlivé činnosti v rámci IT

Outsourcing	Absolutní četnost	Relativní četnost
Internetové připojení	85	84,16
Finanční nebo účetní systém	47	46,53
Správa antivirů/firewallů	40	39,60
Provoz a údržba IS	40	39,60
Vývoj aplikací	35	34,65
Správa lokální sítě nebo správa WAN	32	31,68
Správa databází	28	27,72
Bezpečnostní monitoring	18	17,82

Zdroj: vlastní výzkum

Pozice respondentů, kteří ve výzkumu zastupovali danou organizaci, se lišila. Nejvíce se výzkumu zúčastnili ředitelé či majitelé společností (29,7 %), dále 12,9 % specialistů na oblast IT a 12,9 % vedoucích oddělení. Ostatní pozice byly zastoupeny relativně proporcionálně.

Tabulka 29: Pozice respondenta v rámci výzkumné organizace

Pozice	Absolutní četnost	Relativní četnost
Ředitel, jednatel nebo majitel společnosti	30	29,7
Technik/specialista/řadový zaměstnanec	13	12,9
Vedoucí oddělení	13	12,9
Jiné	9	8,9
Ekonomický nebo finanční ředitel	7	6,9
Manažer bezpečnosti informačních systémů / informačních technologií	7	6,9
Obchodní, technický nebo provozní ředitel	7	6,9
Ředitel informačních systémů / informačních technologií	5	5,0
Specialista bezpečnosti informačních systémů / informačních technologií	5	5,0
Specialista informačních systémů / informačních technologií	3	3,0
Vedoucí oddělení informačních systémů / informačních technologií	2	2,0
Celkem	**101**	**100,0**

Zdroj: vlastní výzkum

Tabulka 30: Jiné pozice respondentů v rámci výzkumné organizace

Jiné pozice	Absolutní četnost
Analytik	1
Referent	1
Řadový zaměstnanec	1
Ředitel řízení kreditních a operačních rizik	1
Ředitel vědeckého ústavu	1
Spolumajitel firmy	1
Starosta města	1
Vedoucí katedry	1
Zástupce ředitele	1
Celkem	**9**

Zdroj: vlastní výzkum

Celkovou bezpečností informací v organizaci se ve většině případů nejvíce zabývá nejvyšší vedení (29,7 %). Jedná se většinou (50,0 %) o malé organizace, dále z 27,6 % o velké organizace. Dále je využívána nejvíce funkce manažera IT (19,8 %) a specialistů na nemanažerské pozici (13,9 %). U malých organizací většinou neexistuje žádná pozice, která se danou oblastí zabývá, což je v souladu s výsledky, že malé organizace se danou oblastí nezabývají.

V terciálním sektoru se nejvíce oblastí bezpečnosti informací zabývá nejvyšší vedení (29,7 %), dále 20,3 % organizací v tomto sektoru má manažera IT či z 13,5 % specialistu na nemanažerské pozici. V sekundárním sektoru je to ve 41,7 % případů pozice v nejvyšším managementu či manažer IT (23,5 %). V případě, že se oblastí zabývají v primárním sektoru, jedná se o manažera na úrovni divize/útvaru/odboru.

S ohledem na velikost organizace lze konstatovat, že ve velkých organizacích existuje pozice manažera IT (33,3 %), případně se zapojuje nejvyšší management (20,5 %). U středních organizací se jedná o nejvyšší vedení (29,2 %) a manažer IT (20,8 %). U malých organizací je to nejvyšší management (majitel organizace) z 39,5 % či neexistuje žádná pozice (31,6 %).

6. 1. 7 Shrnutí výsledků kvantitativního výzkumu

Pro zajišťování bezpečnosti informací organizace nejčastěji využívají *zákonné normy* nezávisle na sektoru a velikosti organizace a *vlastní interní směrnice a standardy* nezávisle na sektoru. Standardy rodiny *ISO 27000* využívají téměř výhradně organizace z terciálního sektoru a jsou to většinou organizace velké. *Ostatní standardy* na bázi ISO se vyskytují v menšině organizací a jsou to vždy organizace velké. Tato skutečnost může souviset s nízkou dostupností ISO standardů pro menší organizace z finančních důvodů, resp. z důvodu komplexnosti. Lze taktéž očekávat, že minoritní standardy ISO jsou trendově na ústupu a jsou postupně nahrazovány standardem ISO 27000.

V rámci všech organizací lze shrnout, že nejsou aplikovány postupy a standardy na bázi ISO standardů.

Organizace za nejvlivnější považují jednoznačně *lidský faktor* a následně *kvalitu technických prostředků ochrany důvěrnosti, integrity a dostupnosti informací*. Tento výsledek lze očekávat, lidský faktor je dlouhodobě identifikován jako nejkritičtější část informačních systémů a lidé jako prvek informačního systému mají nejvíce zranitelností. Faktor *identifikace rizik pro informace* označovali za vlivný převážně respondenti z organizací v terciálním sektoru nezávisle na velikosti organizace. Faktor bezpečnostní *klasifikace informací*, tedy přiřazení hodnoty a rizika konkrétním informacím, považuje za vlivný převážně střední organizace působící v terciálním sektoru (na sektoru závisí). **Pozice faktoru klasifikace informací ve středu spektra**

vlivnosti však neodpovídá jeho teoretickému významu pro dříve uváděné faktory, protože klasifikace informací jako výstup analýzy rizik by měla být vstupem jak pro identifikaci rizik, tak pro realizaci procesů informační bezpečnosti a aplikaci opatření, tedy nasazení technických prostředků. **Skutečnost, že technické prostředky ochrany jsou vnímány jako vlivnější faktor než klasifikace informací lze interpretovat tak, že technické prostředky jsou dlouhodobě vnímány jako obecně účinné protiopatření nezávisející na chráněných informacích** a jsou zřejmě projevem technické vlny dle Von Solms (2006, s. 165).

Organizace z terciálního sektoru v závislosti na velikosti organizace z větší části označují za vlivné také faktory *monitoring osob* a *měření charakteristik informačního systému*. *Měření bezpečnostních charakteristik informací* je v terciálním sektoru vnímáno také jako vlivný faktor (u 90,9 %) nezávisle na velikosti organizace a sektoru. Faktory měření bezpečnosti (informačních systémů i informací) považuje za vlivné především velká organizace v terciálním sektoru. Vliv těchto faktorů je však považován za nejmenší. **Vnímání kvantitativního hodnocení bezpečnosti informací (měření) jako nejméně vlivného faktoru potvrzuje trvání nízké prioritě měření v současné bezpečnostní praxi** dle Doucek (2011, s. 112). V komparaci s faktorem monitoringu osob a technických prostředků je považován za faktor s nižším vlivem.

Organizace si stanovují priority v oblasti dosahování bezpečnosti informací. Splnění legislativních cílů je pro organizace v ČR nejdůležitější a dále pak splnění personálních cílů. Nejmenší prioritu mají technické cíle, což odpovídá ekonomickému chápání cíle informačního systému.

Výsledky ukázaly, že v současné době **nadpoloviční většina zkoumaných organizací hodnotí informační systémy z pohledu rizika pro hodnotné informace** (58,49 %). Nejčastěji realizují hodnocení bezpečnosti informací organizace v terciálním sektoru (77,4 %) a nejméně organizace v sektoru primárním (3,2 %).

Ty organizace, které informační systém nehodnotí (malé a střední organizace), uváděly nejčastěji důvod, že *předpokládají, že informační systém a informace v něm jsou bezpečné* a *spoléhají na svého dodavatele systému* (29 organizací). Výskyt

uvedeného předpokladu klesá s velikostí organizace a většinou se jedná se o malé organizace. Menší část malých a středních organizací *nezná postupy pro hodnocení* nebo *hodnocení nepovažuje za důležité*.

Organizace, které bezpečnost informací hodnotí, tak provádějí nejčastěji s cílem **identifikovat slabiny a vznikající problémy** (41,5 %). V rámci výzkumu byla prokázána střední závislost mezi hodnocením bezpečnosti informací a velikostí organizace (p-hodnota = 0,000; Cramerovo V = 0,444; střední závislost).

Hodnocení bezpečnosti informací provádí primárně velké organizace nezávisle na sektoru.

Nezávisle na sektoru platí, že s rostoucí velikostí organizace je hodnocení primárně vnímáno jako prostředek pro *identifikaci vznikajících problémů a slabin*. Dále má hodnocení za cíl *zlepšování procesů informační bezpečnosti*, *pokrytí legislativních požadavků*, *potvrzení účinnosti nastavených protiopatření* a nejméně často má za cíl *porozumění bezpečnostním rizikům*. Od hodnocení tedy organizace očekávají schopnost vyhodnocovat trend v charakteristikách bezpečnosti a očekává se, že budou identifikovány slábnoucí prvky zakládající nová rizika.

Měření podle výsledků výzkumu provádí velké organizace v terciálním sektoru. Za metodu měření označuje 76,5 % organizací jimi aplikovaný monitoring procesů a chování lidské obsluhy s cílem identifikovat odchylky od nastavených bezpečnostních politik. Přesně definované charakteristiky měří a vyhodnocuje 17,6 %.

Z výsledků vyplývá, že více než 80 % organizací ve skutečnosti neaplikuje měření bezpečnostních charakteristik informací. Aplikaci monitoringu nelze považovat za jejich měření, neboť monitoring vypovídá o dodržování bezpečnostních politik organizace, resp. schopnosti odhalit jejich porušení (např. porušení pravidla přístupu k informacím, nepovolené přihlášení se k technickému prostředku nebo jeho zneužití, pokus o útok), nemusí však vypovídat o stavu konkrétních informací a rozsahu jejich ohrožení.

Faktorová analýza identifikovala 2 faktory, které mají vliv na bezpečnost informací. Tyto faktory autor interpretuje jako „bezpečnostní procesy“ a „bezpečnostně kritické prvky“.

Shluková analýza identifikovala 7 shluků, které jsou uvedeny v kap. 6. 1. 6.

Důraz na lidský faktor a klasifikaci informací je zřetelný především u organizací v pokročilém stupni rozvoje informační bezpečnosti (organizace, které aplikují některou z norem informační bezpečnosti). Aplikace monitoringu je pak trend pozorovatelný u bezpečnostně rozvinutých organizací se silným finančním zázemím.

Kvantitativní výzkum identifikoval hlavní oblasti zájmu:

- měření jako prostředek hodnocení bezpečnosti informací,
- posílení prostředků pro dosažení legislativních cílů,
- snížení rozdílu v přístupu k hodnocení mezi velkými a malými organizacemi,
- prokazatelné snížení rozdílu ve vnímání rizika pro informační aktiva vlastníkem a zpracovatelem,
- další snižování vystavení informací zranitelnostem lidského faktoru plněním informační potřeby (v malých organizacích bezpečnost informací závisí zásadně na lidském faktoru).
- vyvážení významu podceňované klasifikace informací a přeceňovaných technických opatření.

Uvedené oblasti zájmu byly dále zpřesněny v rámci kvalitativního výzkumu.

6. 2 Kvalitativní výzkum a shrnutí výsledků

Kvalitativní výzkum proběhl u dvou organizací A, B v termínu 26. 9. 2014.

Zástupci organizací společně uvádí, že organizační rizika jsou unikátní, je díky tomu limitován reuse a tedy komoditizace. Jako komodita jsou však jednotlivá protiopatření, což je efektivní.

U organizace A je na projektech menšího rozsahu zřejmá simplifikace bezpečnostních problémů, hlavní výběrové kriterium je cena. Existuje snaha systematizovat správu informačních aktiv přejímáním metodik od mateřské organizace, předchozí pokusy však v několika případech nemají očekávaný přínos. U organizace B dokonce nejsou přímo stanovena informační aktiva ani jejich obchodní hodnota (ani business chain value). Existuje velký rozdíl v povědomí zaměstnanců o aplikaci

bezpečnostních opatření. Snahy o zavedení bezpečnostních opatření většinou naráží na jejich uživatelskou nepřívětivost, které snižují akceptovatelnost informačního systému a které se pak snaží zaměstnanci obejít (příklad: zavedení šifrování USB tokenu začali řešit zaměstnanci posíláním údajů emailem a výměnou přes externí systémy, v konečném důsledku se tedy předpokládá snížení úrovně bezpečnosti). Pomocí informačních kampaní a povinných školení se daří stav zlepšovat, což se poměřuje hladkostí průchodu auditem. Vzhledem k tomu, že audit je namátkový, nemusí zcela vypovídat o celkovém stavu v organizaci B, navíc případná certifikace morálně zastarává (pozbývá validity). Zaměstnanci často podléhají pocitu vlastní nedůležitosti v celkovém systému organizace a neuvědomují si, že mohou být branou k dalším útokům.

Zástupce organizace A uvedl, že chybí pružná adaptivnost na incidenty, změna ve vlastních systémech je dlouhodobá (změna dodavatele, změna infrastruktury, změna procesů, nevytrénovaní zaměstnanci). Je těžké stanovit cíle a dodržet kvalitu parametrů bezpečnostního projektu, resp. technického řešení při tvorbě systému, za provozu. Je pracné a nákladné dodržet kvalitu monitoringu a validitu výsledků měření, současně nejsou dostupní kvalifikovaní pracovníci na analýzu bezpečnostních incidentů. V současnosti panuje obava z Advanced Persitent Threats (APT) z externího prostředí a z rostoucího objemu zcizených dat globálně (viz případy Sony, JP Morgan apod.), přičemž je složité připustit jakýkoliv únik informací. V interním prostředí organizace je těžké rozpoznat oprávněné přístupy v neoprávněném kontextu, což vyžaduje namátkové kontroly a kontrola dodržování workflow. Konvenční postupy informační bezpečnosti závisí na statické ochraně, ale typy útoků se střídají. Další stupeň složitosti vnáší nové technologie.

Hlavní problémový bod je poskytnutí důkazu, že konkrétní data byla kompromitována během detekovaného incidentu, resp. samotná detekce incidentu. Vnímání rizik u zaměstnanců neodpovídá rizikům nastaveným organizací, což umožňuje útočníkům využít rozdílu ve vnímání k lepšímu využití zranitelností. Klasifikace informací a jejich ohodnocení je vnímáno jako podružné.

Kvantitativní výzkum zpřesnil oblast zaměření:

- ochrana informačních aktiv,
- podpora klasifikace informací,
- odlišné vnímání rizik na straně vlastníka (subjektu odpovědného za informace) a zpracovatele (uživatele, systému, dodavatele služby), resp. odlišného cenění hodnoty aktiv.

Na uvedené oblasti byly v rámci disertační práce zaměřeny instrumentální případové studie.

6. 3 Případové studie

Na základě provedeného kvantitativního výzkumu byly identifikovány oblasti zájmu pro výběrový vzorek organizací. Shrnutí viz kap. 6. 1. 7. Provedením kvalitativního výzkumu technikou rozhovorů zaměřené na vybranou oblast rozšířeného bezpečnostního modelu u vybrané organizace A byla tato oblast dále zpřesněna a zaměřena na **„klasifikace informace“** a **„odlišné vnímání rizik ve vztahu vlastník-informace a zpracovatel-informace“**. U organizace B pak na **„snížení vystavení informací zranitelnostem vycházejících z lidského faktoru“**. Shrnutí viz kap. 6. 3. 3.

6. 3. 1 Organizace A

Následuje případová studie pro organizaci A. Organizace A se zúčastnila průzkumu popsaného v kap. 4. 12.

6.3.1.1 Charakteristika organizace A

Organizace A, ve které probíhal výzkum, patří mezi přední bankovní instituce v České republice a v regionu střední a východní Evropy. Lze ji charakterizovat jako univerzální banku se širokou nabídkou služeb pro 1,6 milionů klientů v oblasti retailového, podnikového a investičního bankovnictví a je dostupná prostřednictvím sítě 399 poboček, přímého bankovnictví a vlastní distribuční sítě. Strategií organizace je spojení finanční stability se strategií udržitelného rozvoje. Jejím posláním je zastávat referenční pozici v oblasti bankovnictví orientovaného na obsluhování klientů, být uznávanou bankou na svých trzích, být nablízku svým zákazníkům, kteří si danou společnost vybírají díky její kvalitě služeb a nasazení jejích pracovních týmů.

Charakteristika organizace dle ČSÚ:

- Sektor: Terciální sektor (oblast bankovnictví).
- Velikost organizace: Velká společnost (nad 250 zaměstnanců), průměrný počet zaměstnanců každoročně přesahuje 8 500.
- Vlastnictví organizace: společnost s většinovým zahraničním podílem.

Závěr z kvalitativního výzkumu (rozhovorů): Přístup k řízení informační bezpečnosti v dané organizaci odpovídá modelu utopené bezpečnosti.

6.3.1.2 Popis situace

Dynamika vnitřního prostředí organizace na operativní úrovni, tj. změny ve vývojových procesech, v lidských zdrojích a jejich znalostech a přístupech k vývoji, v počítačových nástrojích používaných pro vývoj a tlak na rychlý rozvoj produktu znamenají neustálé změny zakládající nová neidentifikovaná rizika. Obecným problémem při vývoji zpracovávající webové aplikace v organizaci A je identifikovat rozdíly mezi primárními, vlastníkem identifikovanými a oklasifikovanými sadami informací definovanými v analytické fázi, a skutečnými sadami informací používanými ve finálním produktu a jeho následujících verzích. Princip penetračního testování selhává v této oblasti a projevuje se opakovaným výskytem neklasifikovaných informací, neboť penetrační testování není zaměřováno na identifikaci těchto rozdílů.

6.3.1.3 Analýza situace

Problém v dané organizaci vyplývá z problému nedostatečné schopnosti „uzavření objektu“ (angl. confinement) – primárně informací a dat využívaných v aplikační logice. Příčinou je nedostatečná aplikace opatření „dlouhodobé informování uživatelů o nutnosti zvláštního zacházení“ a jeho prosazování v rámci vývoje webových aplikací. Vlastník (zodpovědný subjekt) deleguje zpracování těchto dat a informací (objektů) na vývojový tým a zrací tím tak kontrolu nad informačními toky těchto aktiv ve finální aplikaci. Ochrana je pak v principu záležitostí vyvinuté aplikace a zůstává vlastníkovi skryta v aplikačním designu. Vlastník je nucen spolehnout se na skutečnost, že systém jako celek chrání všechny i odvozená informační aktiva. Možnosti bezpečnostního testování aplikace formou penetračních testů využívají black-box přístup a v identifikaci komplexnějších informací neposkytují dostatečnou efektivitu a dlouhodobě nevyrovnané výsledky. V tomto případě v reálu nastává situace, že díky časovým podmínkám projektu je vlastník nucen akceptovat rizika.

Cílem měření je detekovat rozdíly mezi očekávaným způsobem nakládání s klasifikovanými daty v aplikaci vyplývajícím z návrhu a reálným informačním tokem v aplikaci. Předmětem detekce je konkrétní vyvíjená webová aplikace v Přímém bankovnictví. Detekované rozdíly umožní včasnou korekci případného nepříznivého stavu.

6.3.1.4 Výsledky

Navrženým konceptuálním postupem vývoje sady měr pomocí nástroje GQM (kap. 5. 4) vznikla následující sada výstupů:

Konstrukt měření podle GQM je definován takto:

GOAL (Cíl)	Dlouhodobě identifikovat všechny vlastníkem (E3) klasifikované (E2) informace (E1), které jsou zpracovávány, ukládány a přenášeny (E4) v rámci inhouse vyvíjených webových aplikací neidentifikovaným/neautorizovaným zpracovatelem/útočníkem (E4).
QUESTION (Otázka)	Kolik informací je v konkrétní aplikaci zpracováváno v rozporu s přístupovými oprávněními definovanými vlastníkem?
METRIC (Míra)	(1) Počet datových elementů z datového modelu aplikace, které jsou přenášeny na klientskou stanici. (2) Počet datových elementů z datového modelu aplikace, které jsou na klientské stanici zobrazovány a zpracovávány neautorizovaným subjektem. (3) Počet datových elementů z datového modelu aplikace, které jsou přenášeny a nejsou zobrazovány ani zpracovávány. (4) Počet datových elementů, které jsou zobrazovány a zpracovány autorizovaným subjektem

GOAL (Cíl)	Dlouhodobě snížit počet vlastníkem (E3) neoklasifikovaných (E2) informací (E1), které jsou zpracovávány, ukládány a přenášeny (E4) v rámci inhouse vyvíjených webových aplikací.
QUESTION (Otázka)	Kolik neoklasifikovaných informací je v konkrétní aplikaci ukládáno, zpracováváno a přenášeno?
METRIC (Míra)	(1) Počet datových elementů z datového modelu aplikace, které jsou přenášeny na klientskou stanici. (2) Počet datových elementů z datového modelu aplikace (včetně vývojových), které nemají přiřazenu klasifikaci a zpracovávány na klientské stanici a přenášeny na ni.

Použitý měřicí konstrukt a analytický model je uveden v příloze v kap. 10. Pro účely měření byl aplikován experimentální nástroj s pracovním názvem Web Application Reference Monitor Observer (WA-RMO), který byl pro účely této práce implementován. Detailnější popis nástroje je uveden v příloze v kap. 10. 7 a detailní informace o průběhu měření uvádí Tabulka 31.

Tabulka 31: Sada konstruktů G1 a G2 pro organizaci A

ID	Goal	Question	Oblasti rozšířeného bezpečnostního modelu	Zkoumaná vazba	Metric	Konstrukt měření dle GQM	Konstrukt měření dle ISO 27004	Počet iterací vývoje míry	Počet měřících cyklů	Průměr trvání iterace vývoje míry [den]	Míra validována vlastníkem	Míra akceptována vlastníkem
G1	Dlouhodobě identifikovat všechny vlastníkem (E3) klasifikované (E2) informace (E1), které jsou zpracovávány, ukládány a přenášeny (E4) v rámci inhouse vyvíjených webových (E4).	Q1 Kolik informací je v konkrétní aplikaci zpracováváno v rozporu s přístupovými oprávněními definovanými vlastníkem.	E1, E2, E3, E4	E4 - E1	G1_Q1_M: web application information leakage	*KB_GQMC_G1_v5.docx*	*KB_ISO2004C_G1_v2.docx*	5	5	14	A	A
G2	Dlouhodobě snížit počet vlastníkem (E3) neoklasifikovaných (E2) informací (E1), které jsou zpracovávány, ukládány a přenášeny (E4) v rámci inhouse vyvíjených webových aplikací.	Q1 Kolik neoklasifikovaných informací je v konkrétní aplikaci ukládáno, zpracováváno a přenášeno.	E1, E2, E3, E4	E3 - E1	G2_Q1_M: web application information classification coverage	*KB_GQMC_G2_v3.docx*	*KB_ISO2004C_G2_v1.docx*	3	5	5	A	A

Zdroj: vlastní zpracování

Tabulka 32: Průběh vývoje a měřicích cyklů v organizaci A pro G1

Verze konstruktu	Měřící cyklus #	Začátek	Konec	Trvání [den]	Metoda měření	m1**	m2**	m3	m4**	I1	G1_Q1_M: web application information leakage	*I1*
3	**0***	20.10.2014	24.10.2014	4	WA-RMO	27	0	0	27	0 < G2_Q1_M < 0,05	0,00	+
4	**1**	27.10.2014	31.10.2014	11	WA-RMO	35	0	1	34	0 < G2_Q1_M < 0,05	0,00	+
5	**2**	10.11.2014	14.11.2014	18	WA-RMO	35	1	0	35	0 < G2_Q1_M < 0,05	0,03	+
-	**3**	17.11.2014	21.11.2014	11	WA-RMO	35	0	0	35	0 < G2_Q1_M < 0,05	0,00	+
-	**4**	1.12.2014	5.12.2014	18	WA-RMO	37	2	0	35	0 < G2_Q1_M < 0,05	0,05	+
-	**5**	15.12.2014	19.12.2014	18	WA-RMO	37	1	0	35	0 < G2_Q1_M < 0,05	0,03	+
* 0. měřící cyklus je pilotní												
** Public klasifikace není zahrnuta												

Zdroj: vlastní zpracování

Tabulka 33: Průběh vývoje a měřicích cyklů v organizaci A pro G2

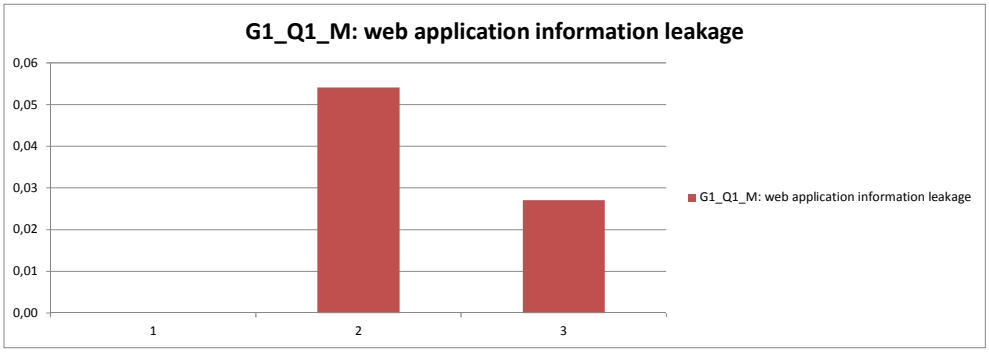
Verze konstruktu	Měřící cyklus #	Začátek	Konec	Trvání [den]	Metoda měření	m1**	m2**	m3	I1	G2_Q1_M: web application information classification coverage	*I1*
1		8.5.2014	3.10.2014	148	Formální thread Model podle metodiky MS SDLC	15	15	0	0,5 < G2_Q1_M < 1	1,00	+
2		6.10.2014	10.10.2014	4	Penetrační tester	22	17	0	0,5 < G2_Q1_M < 1	0,77	+
3	**0***	20.10.2014	24.10.2014	18	WA-RMO	27	17	1	0,5 < G2_Q1_M < 1	0,63	+
4	**1**	27.10.2014	31.10.2014	11	WA-RMO	25	17	-2	0,8 < G2_Q1_M < 1	0,68	--
5	**2**	10.11.2014	14.11.2014	18	WA-RMO	25	22	-	0,8 < G2_Q1_M < 1	0,88	-
-	**3**	17.11.2014	21.11.2014	11	WA-RMO	23	23	-	0,8 < G2_Q1_M < 1	1,00	+
-	**4**	1.12.2014	5.12.2014	18	WA-RMO	23	23	-	0,8 < G2_Q1_M < 1	1,00	+
-	**5**	15.12.2014	19.12.2014	18	WA-RMO	28	23	-	0,8 < G2_Q1_M < 1	0,82	--
* 0. měřící cyklus je pilotní											
** Public klasifikace není zahrnuta											

Zdroj: vlastní zpracování

6.3.1.5 Vyhodnocení G1_Q1_M

Průběh odvozené míry G1_Q1_M v rámci vývojového cyklu míry je uveden v následujícím obrázku. Odvozená míra je pojmenována jako „Web application information leakage“ a stanovuje poměr datových elementů, na které bylo přistoupeno/nebo nebyly zobrazeny korektně ve výsledné stránce k celkovému počtu identifikovaných datových elementů odesílaných ze serverové strany na klientskou. Rozsah indikátoru byl nastaven na 0-5%. Míry m3 a m4 jsou kontrolními mírami, které poskytoval WAR-RMO mechanismus.

Graf 7: Časová řada hodnot míry „Web application information leakage“ v iteracích vývoje



Zdroj: vlastní zpracování

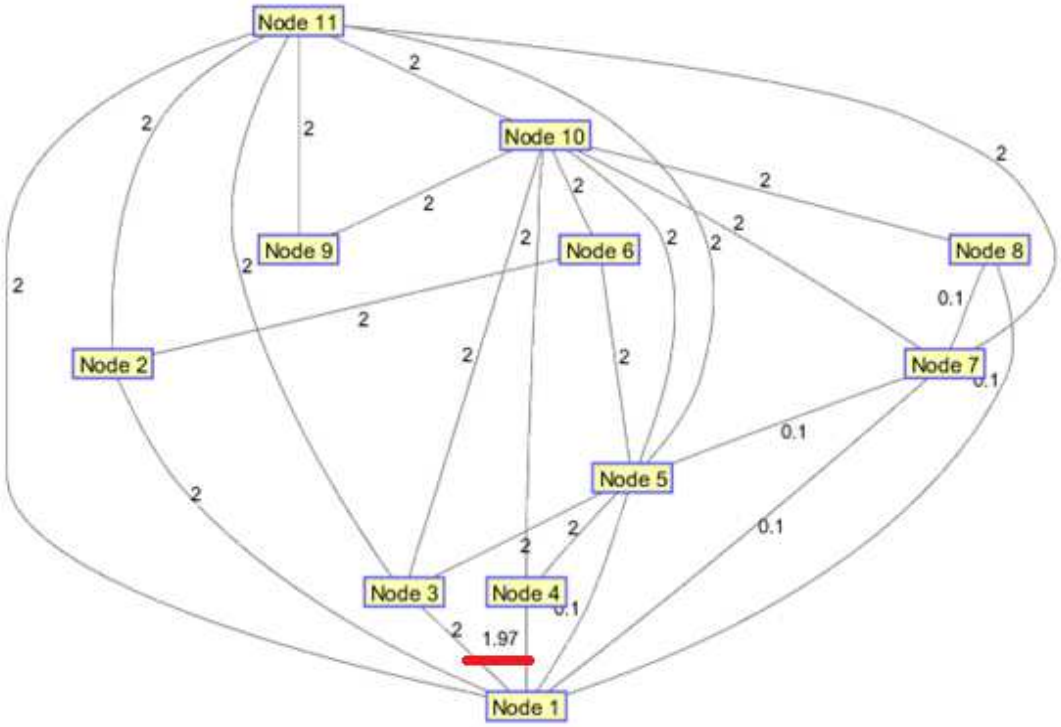
Měřicí funkce odvozené míry G1_Q1_M je definována jako:

$$\mu_{G1_{Q1}} = \frac{m2}{m1}$$

a přímo produkuje relativní hodnoty. Byl přímo použit do výpočtu váhy hrany E(4, 1) s iniciální vlastní vahou $w(G1\_Q1\_M) = 1$. Indikátor byl v poslední iteraci nastaven na interval <0;0,05>. Dopad na ohodnocení síly vazby „Zpracovatel cení informace“ v poslední iteraci vývoje míry a tedy akceptaci míry je:

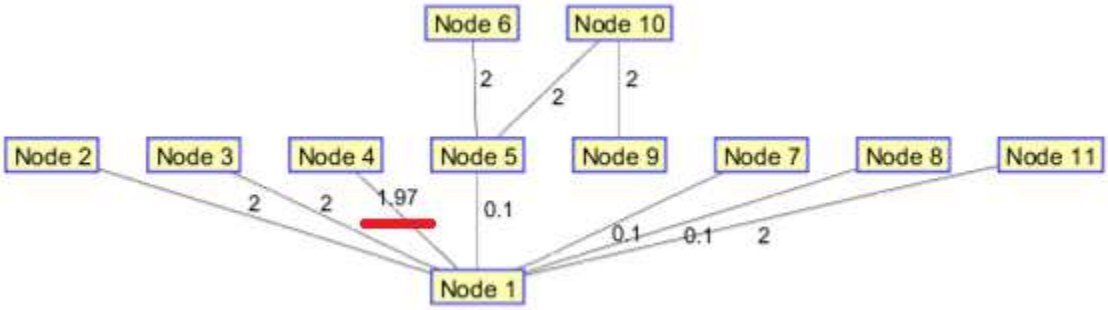
$$w(E_{4,1}) = \frac{\sum_{i=1}^{m} \mu_{Ri}.W(\mu_i)}{\sum_{i=1}^{m} W(\mu_i)} = \frac{(1-0{,}03).1}{1} = 0{,}97$$ (Zdroj: vlastní výpočet)

Graf 8: Ohodnocení grafu se zahrnutou mírou G1_Q1_M



Zdroj: vlastní zpracování

Graf 9: Nejmenší kostra grafu se zahrnutou mírou G2_Q1_M



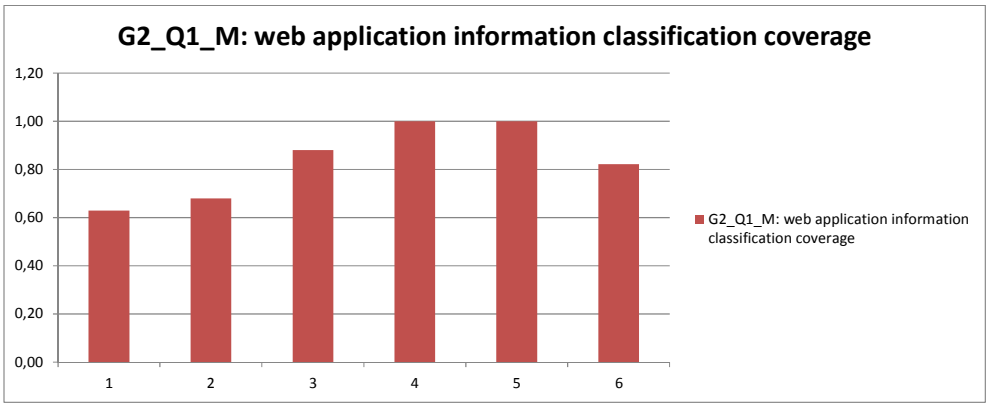
Zdroj: vlastní zpracování

Podle očekávání transformace do nejmenší kostry grafu přímo označila tuto vazbu jako slabou.

6.3.1.6 Vyhodnocení G2_Q1_M

Průběh odvozené míry G2_Q1_M v rámci vývojového cyklu míry je uveden v následujícím obrázku. V průběhu cyklů byly upřesňovány parametry WA-RMO a nastavený indikátor. Nastavená dolní hodnota indikátoru 0,5 se ukázala jako nedostatečná, protože systém vždy generoval míru v jeho rozsahu.

Graf 10: Časová řada hodnot míry „Web application information classification coverage“ v iteracích vývoje



Zdroj: vlastní zpracování

V prvních dvou vývojových iteracích byla sledována i míra „m3: změna v počtu pracovníků vývojového týmu, který na vyvíjené aplikaci pracoval“. Protože se však nepodařilo identifikovat závislost na této míře, nebyla její hodnota do odvozené míry započítávána.

Měřicí funkce míry G2_Q1_M je definována jako:

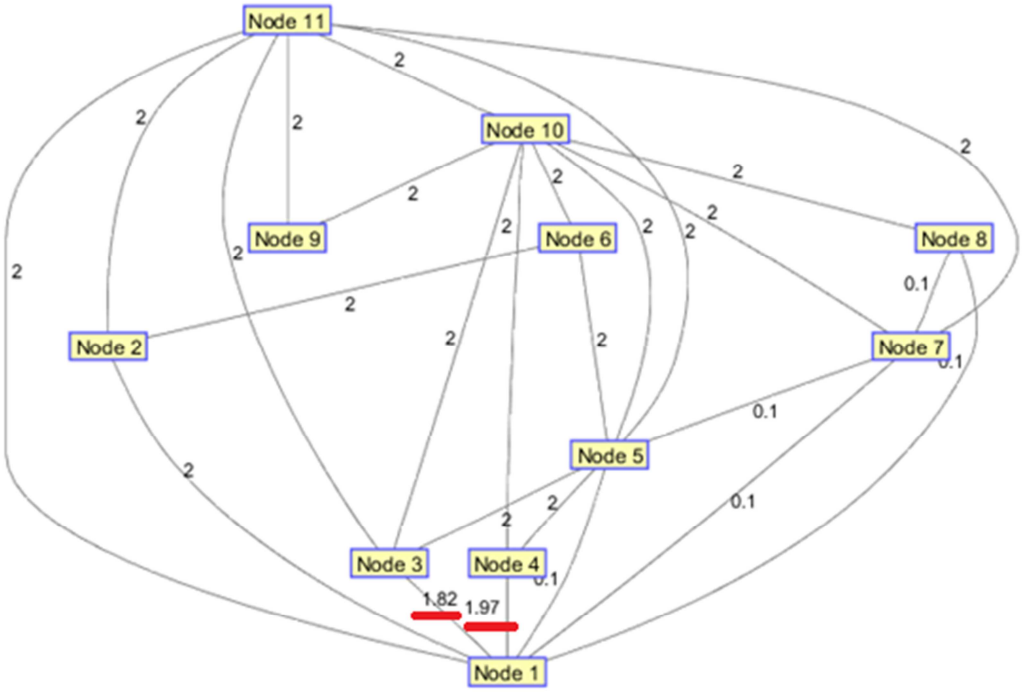
$$\mu_{G2_{Q1}} = \frac{m2}{m1}$$

přímo produkuje relativní hodnoty. Byl přímo použit do výpočtu váhy hrany E(3, 1) s iniciální vlastní vahou $w(G2\_Q1\_M) = 1$. Tedy dopad na ohodnocení síly vazby „Vlastník cení informace“ v poslední iteraci vývoje míry a tedy akceptaci míry je:

$$w(E_{3,1}) = \frac{\sum_{i=1}^{m} \mu_{Ri}.W(\mu_i)}{\sum_{i=1}^{m} W(\mu_i)} = \frac{0{,}82.1}{1} = 0{,}82$$ (Zdroj: vlastní výpočet)

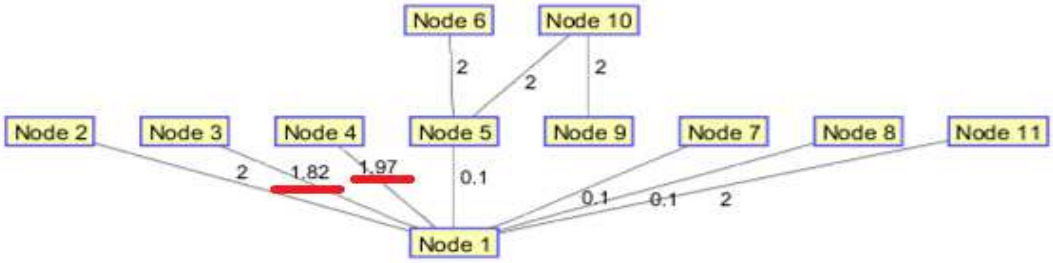
Transformace do nejmenší kostry grafu přímo označila tuto relaci jako slabou (viz Graf 11 a Graf 12).

Graf 11: Ohodnocení grafu se zahrnutou mírou G2_Q1_M



Zdroj: vlastní zpracování

Graf 12: Nejmenší kostra grafu se zahrnutou mírou G2_Q1_M



Zdroj: vlastní zpracování

6.3.1.7 Prezentace bezpečnostní pozice informačního systému

Bezpečnostní pozice informačního systému vyplývající z naměřených hodnot je

$$BP_{IS}\,(I, t_5) = (1; 0{,}82; 0{,}97; -1; 1; -1; -1; 1; 1; 1)$$

kde:

I … klasifikované informace a data z datového modelu webové aplikace.

t_5 … pátá iterace měření (viz Tabulka 32 a Tabulka 33).

Uvedená hodnota platí při redukci ochranných opatření a v tomto případě je definována jako celá množina MO_V s výjimkou třídy KLASIF_RIZ_INF a RIZ_PRISTUP.

Vypočtené hodnoty kritických bezpečnostních charakteristik při V_{TO}*(RIZ_PRISTUP)=(2,5; 2,5; 1,5)* a V_{TO} *(KLASIF_RIZ_INF) = (2,5; 2; 1)*:

$$C(I, t_5) = \frac{0{,}97.2{,}5 + 0{,}82.2{,}5}{2{,}5 + 2{,}5} = \frac{2{,}425 + 2{,}05}{5} = \frac{4{,}475}{5} = 0{,}895$$

$$I(I, t_5) = \frac{0{,}97.2{,}5 + 0{,}82.2}{2{,}5 + 2} = \frac{2{,}425 + 1{,}64}{4{,}5} = \frac{4{,}065}{4{,}5} = 0{,}903$$

$$A(I, t_5) = \frac{0{,}97.1{,}5 + 0{,}82.1}{1{,}5 + 1} = \frac{1{,}455 + 0{,}82}{2{,}5} = \frac{2{,}275}{2{,}5} = 0{,}91$$

Výsledek hodnocení bezpečnosti informace I v informačním systému v čase t_5 (dne 19.12.2014) je definován takto:

Odhad charakteristik systému pro C(I, t_5) = 0,895; I(I, t5) = 0,903; A(I, t_5) = 0,91. Jedná se o relativně vysoké hodnoty ukazující na vysokou kvalitu procesu „řízení přístupu ve webové aplikaci“ s nízkým indikátorem „Web Application Information Leakage“ a procesu „klasifikace informací“ vysokým „Web Application Information Clasification Coverage“.

Je třeba zohlednit, že měření proběhlo při velmi vysoké redukci ochranných opatření, tj. bez dalších informací o dalších měřených charakteristikách informačního systému, protože se měření zaměřilo na webovou přístupovou vrstvu aplikace. Znamená to, že případné úniky dat a informací jiným kanálem (přes databázovou vrstvu, uživatelem na pracovní stanici apod.) nejsou v měření podchyceny a hodnoty C, I, A jsou s ohledem na architekturu aplikace neúplné. Neúplnost je v hodnocení vyjádřena vysokou redukcí ochranných opatření.

Validace výsledků měření proběhla s odpovědným pracovníkem v každé iteraci měření. Prezentované hodnoty bezpečnostní pozice byly ve všech kolech kvalitativně ověřeny a prohlášeny za odpovídající skutečnosti. Byly také navrženy korekce do parametrů a průběhu měření.

6. 3. 2 Organizace B

Následuje případová studie pro organizaci B. Organizace B se zúčastnila průzkumu popsaného v kap. 4. 12.

6.3.2.1 Charakteristika organizace

Organizace B, ve které probíhal výzkum, patří mezi přední organizace v oblasti IT konzultací a služeb pro dopravu, poštovní služby a logistiku, energetiku a síťová odvětví, finanční služby, Oil and Gas, průmysl a výrobu, Retail a služby a v neposlední řadě telekomunikace a média. Společnost je držitelem certifikátu Systému řízení bezpečnosti informací (ISMS) podle mezinárodní normy ISO/IEC 27001:2013 pro obor: Konzultační služby, systémová integrace a služby v oblasti outsourcingu IT a firemních procesů a je prověřena Národním bezpečnostním úřadem na seznamování se s utajovanými informacemi stupně utajení „TAJNÉ" ve smyslu zákona č. 412/2005 Sb.

Charakteristika organizace dle ČSÚ:

- Sektor: Terciální sektor (oblast systémové integrace).
- Velikost organizace: Velká společnost (nad 250 zaměstnanců), průměrný počet zaměstnanců každoročně přesahuje 600.
- Vlastnictví organizace: společnost s většinovým zahraničním podílem.

Přístup k řízení informační bezpečnosti odpovídá modelu odtržené bezpečnosti.

6.3.2.2 Popis situace

V organizaci B je sledována schopnost pracovníků zajistit dodržování bezpečnostní politiky jiné odběratelské organizace při nakládání se všemi typy informačních aktiv. Cílem je udržet důvěrnost a integritu informací na operativní úrovni v úrovni nastavené odběratelskou organizací. Bylo zjištěno několik incidentů, kdy důvěrné informace byly odesílány přes emailový systém.

6.3.2.3 Analýza situace

Problém v dané organizaci vyplývá opět z problému nedostatečné schopnosti „uzavření objektu“ (angl. confinement) – primárně informací a dat odesílaných uživateli emailovým kanálem.

Při dosahování cíle snížení počtu incidentů bylo zvoleno modelování cílového chování uživatele jako obecného prvku informačního systému, od něhož je vyžadováno chování kvalitativně blížící se TCB, tj. chování odpovídající reference monitoru. Pro zajištění chování na úrovni TCB musí být saturována informační potřeba uživatelů tak, aby:

- vždy měli přístup k aktuálnímu stavu autorizační databáze a klasifikace informací,
- vždy měli jednoznačnou důvěryhodnou identitu subjektu, se kterým komunikují,
- bylo možno auditovat jejich chování a přístup k emailu subjektem.

6.3.2.4 Výsledky

Navrženým konceptuálním postupem vývoje sady měr pomocí nástroje GQM (kap. 5. 4) vznikla následující sada výstupů:

Konstrukt měření podle GQM je definován takto:

GOAL (Cíl)	Dlouhodobě zajistit, aby zpracovatel informace (E4) identicky cenil hodnotu (E2) informace (E1) přenášené kanálem email a aplikoval stejná opatření, jaká vynucuje vlastník (E3) při komunikaci emailem.
QUESTION (Otázka)	Kolik odeslaných emailů není označeno požadovanou bezpečnostní klasifikací? Kolik emailů není ochráněno před odesláním?
METRIC (Míra)	(1) Počet emailů odeslaných na vybranou podmnožinu adres bez přiřazené klasifikace a ochrany. (2) Kolik takových emailů je odesláno na subjekt, který nemá přiřazenu identitu v autorizační databázi? (3) Počet odesílajících zaměstnanců.

Použitý měřicí konstrukt je uveden v kap. 10. Pro účely měření byl aplikován experimentální nástroj emailSecurityAdvisor. Tento nástroj poskytuje prostředky ochrany emailové zprávy na principu infrastruktury veřejných klíčů a šifrování v závislosti na přiřazené klasifikaci.

Tabulka 34: Sada konstruktů G1 pro organizaci B

ID	Cíl (Goal)	Otázka (Question)	Oblasti rozšířeného bezpečnostního modelu	Zkoumaná vazba	Míra (Metric)	Konstrukt měření dle GQM	Konstrukt měření dle ISO 27004	Počet iterací vývoje míry	Počet měřicích cyklů	Průměr. trvání iterace vývoje míry [den]	Míra validována vlastníkem	Míra akceptována vlastníkem
G1	Dlouhodobě zajistit, aby zpracovatel informace (E4) identicky cenil hodnotu (E2) informace (E1) a aplikoval stejná opatření, jaká vynucuje vlastník (E3) při komunikaci emailem.	Q1 kolik údajů je odesláno emailem bez správné klasifikace ?	E1, E2, E3, E4	E4 - E1 E3 - E1	G1_Q1_M email application leakage	*CGI_GQMC_G1_v2.docx*	*CGI_ISO2004C_G1_v1.docx*	19,33	12	14	A	A

Zdroj: vlastní zpracování

Tabulka 35: Průběh vývoje a měřicích cyklů v organizaci B pro G1

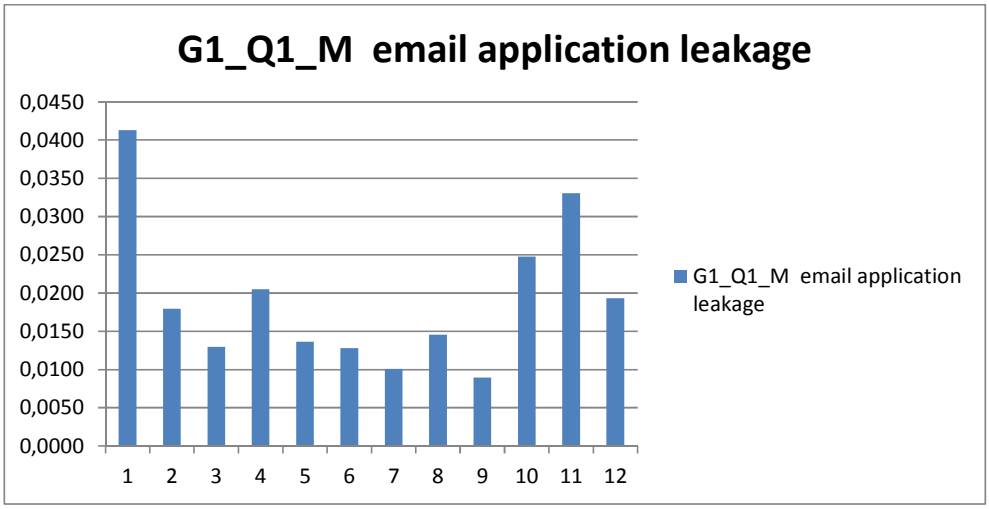
Verze konstruktu	Měřící cyklus #	Začátek	Konec	Trvání [den]	Metoda měření	m1	m2	m3	I1	G1_Q1_M email application leakage	*I1 email application information leakage*
1	1	5.1.2015	6.2.2015	32	Email Security advisor+audit trail	3815	315	2	0 < G2_Q1_M < 0,02	0,0413	+
	2	9.2.2015	6.3.2015	25	Email Security advisor+audit trail	2999	269	5	0 < G2_Q1_M < 0,02	0,0179	--
	3	9.3.2015	10.3.2015	1	Email Security advisor+audit trail	103	4	3	1 < G2_Q1_M < 0,02	0,0129	-
	4	10.3.2015	11.3.2015	1	Email Security advisor+audit trail	122	5	2	2 < G2_Q1_M < 0,02	0,0205	---
	5	11.3.2015	12.3.2015	1	Email Security advisor+audit trail	110	3	2	3 < G2_Q1_M < 0,02	0,0136	--
	6	12.3.2015	13.3.2015	1	Email Security advisor+audit trail	130	5	3	4 < G2_Q1_M < 0,02	0,0128	---
	7	13.3.2015	14.3.2015	1	Email Security advisor+audit trail	99	2	2	5 < G2_Q1_M < 0,02	0,0101	-
	8	16.3.2015	17.3.2015	1	Email Security advisor+audit trail	103	3	2	6 < G2_Q1_M < 0,02	0,0146	--
	9	17.3.2015	18.3.2015	1	Email Security advisor+audit trail	112	1	1	7 < G2_Q1_M < 0,02	0,0089	o
	10	18.3.2015	19.3.2015	1	Email Security advisor+audit trail	121	3	1	8 < G2_Q1_M < 0,02	0,0248	----
	11	19.3.2015	20.3.2015	1	Email Security advisor+audit trail	121	4	1	9 < G2_Q1_M < 0,02	0,0331	-----
	12	20.3.2015	21.3.2015	1	Email Security advisor+audit trail	155	3	1	10 < G2_Q1_M < 0,02	0,0194	----

Zdroj: vlastní zpracování

6.3.2.5 Vyhodnocení G1_Q1_M

Průběh odvozené míry G1_Q1_M v rámci vývojového cyklu míry je uveden v následujícím obrázku. Odvozená míra je pojmenována jako „average email application leakage per user“ a stanovuje poměr emailových zpráv, které byly odeslány bez přiřazené klasifikace k celkovému počtu odeslaných zpráv. Rozsah indikátoru byl nastaven na 0-2%.

Graf 13: časová řada hodnot míry „email application leakage“ v iteracích vývoje



Zdroj: vlastní zpracování

Analytický model míry G1_Q1_M

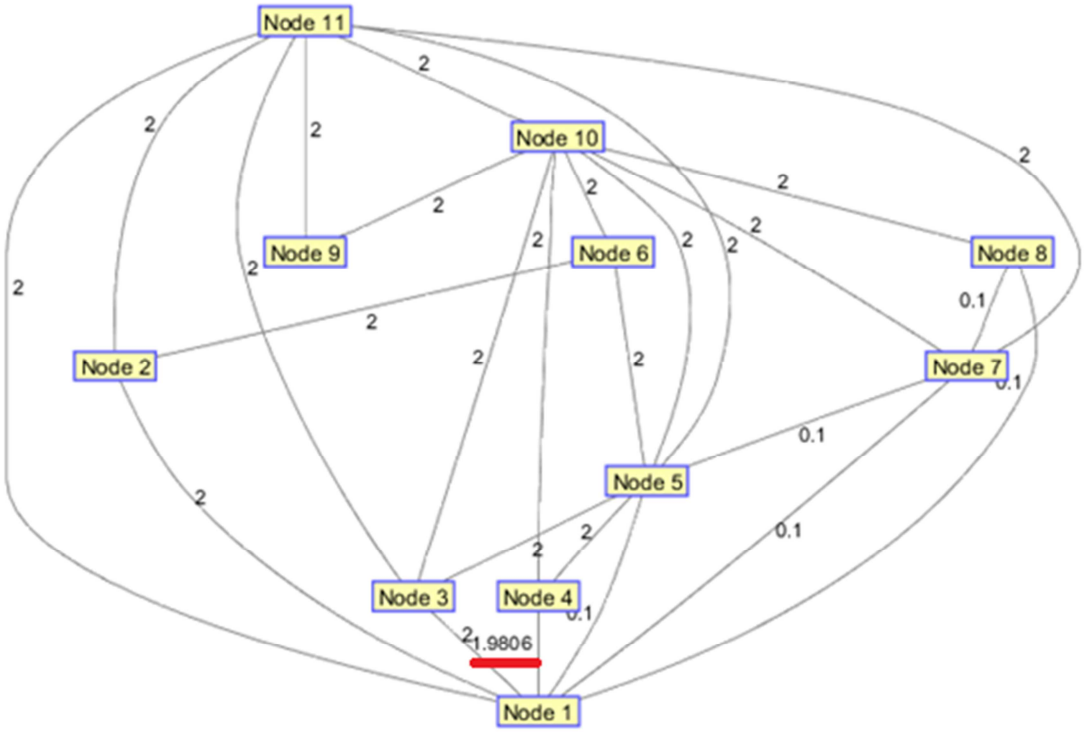
$$\mu_{G1_{Q1}} = \frac{\frac{m2}{m1}}{m3}$$

přímo produkuje relativizované hodnoty. Byl přímo použit do výpočtu váhy hrany E(4, 1) s iniciální vlastní vahou $w(G1\_Q1\_M) = 1$. Tedy dopad na ohodnocení síly vazby „Zpracovatel cení informace“ v poslední iteraci vývoje míry a tedy akceptaci míry je:

$$w(E_{4,1}) = \frac{\sum_{i=1}^{m} \mu_{Ri}.W(\mu_i)}{\sum_{i=1}^{m} W(\mu_i)} = \frac{(1-0{,}0194).1}{1} = 0{,}9806$$ (Zdroj: vlastní výpočet)

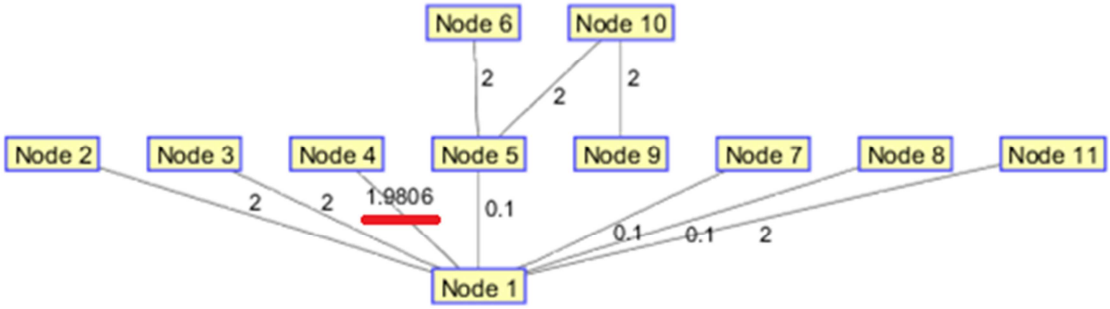
Nestabilní průběh míry v jednotlivých měřicích intervalech ukazuje na náhodný jev v přiřazování klasifikace odesílaným emailům. Dalším zkoumáním bylo zjištěno, že odesílatelé v případě, že nejsou ochotni klasifikaci zjišťovat, resp. zjišťovat komu je možné email odeslat, použijí nejvyšší stupeň klasifikace, což řeší ochranu, pravděpodobně však komplikuje komunikaci na větší množinu osob.

Graf 14: Ohodnocení grafu se zahrnutou mírou G1_Q1_M



Zdroj: vlastní zpracování

Graf 15: Nejmenší kostra grafu se zahrnutou mírou G1_Q1_M



Zdroj: vlastní zpracování

Transformace do nejmenší kostry grafu přímo označila tuto vazbu jako slabou.

6.3.2.6 Prezentace bezpečnostní pozice informačního systému

Bezpečnostní pozice informačního systému je

$$BP_{IS}\ (I, t_5) = (1; 1; 0{,}9806; -1; 1; -1; -1; 1; 1; 1)$$

kde:

I … klasifikované informace přenášené emailovým systémem.

t_{12} … dvanáctá iterace měření (viz Tabulka 35).

Uvedená hodnota platí při redukci ochranných opatření MO_V bez opatření RIZ_PRISTUP.

Vypočtené hodnoty kritických bezpečnostních charakteristik při $V_{TO}(RIZ\_PRISTUP)=(2{,}5; 2{,}5; 1{,}5)$:

$$C(I, t_{12}) = \frac{0{,}9806.2{,}5}{2{,}5} = 0{,}9806$$

$$I(I, t_{12}) = \frac{0{,}9806.2{,}5}{2{,}5} = 0{,}9806$$

$$A(I, t_{12}) = \frac{0{,}9806.1{,}5}{1{,}5} = 0{,}9806$$

Výsledek hodnocení bezpečnosti informace I v informačním systému v čase t_{12} (dne 20.3.2015) je definován takto:

Odhad charakteristik systému pro $C(I, t_{12}) = I(I, t_{12}) = A(I, t_{12}) = 0{,}9806$.

Jedná se také o relativně vysoké hodnoty ukazující na vysokou kvalitu procesu „řízení přístupu k odesílaným emailům“ s nízkým indikátorem „Email Application Information Leakage“.

Měření proběhlo při velmi vysoké redukci ochranných opatření, tj. taktéž bez dalších informací o dalších měřených charakteristikách informačního systému, protože se měření zaměřilo na vazbu „Zpracovatel (odesílatel) cení informace“. Znamená to, že případné úniky emailů a informací jiným kanálem (kopií souborů na přenosný disk, vytištění uživatelem na papír apod.) nejsou v měření podchyceny a hodnoty C, I, A jsou s ohledem na celý informační systém neúplné. Neúplnost je v hodnocení popsána vysokou redukcí ochranných opatření.

Validace výsledků měření proběhla s rolemi, které hodnotily akceptovatelnost měr (CISO) v každé iteraci měření. Prezentované hodnoty bezpečnostní pozice byly ve všech kolech kvalitativně ověřeny a prohlášeny za odpovídající skutečnosti. Byly také navrženy korekce do parametrů a průběhu měření.

6. 3. 3 Shrnutí výstupů z případových studií

Proces hodnocení bezpečnosti informace navrženým postupem ukázal především silnou stránku grafické prezentace pozice informačního systému pro logickou skupinu „klasifikovaná data“ a „klasifikované emaily“. Pozitivně působí možnost posoudit sílu vazby a schopnost reagovat v oblasti lidských zdrojů (zpracovatel) např. školením. Pozitivní vliv na schopnost stanovovat cíle má taktéž použitý rozšířený konceptuální model, který minimálně v oblasti zkoumaných relací transformovaných do charakteristik systému působí jako efektivní nástroj pro stanovení cílů a otázek ve formě návrhu, což následně usnadňuje identifikací míry, což je v souladu s cílem práce.

Problematickou se jeví aplikace samotného **vývoje míry**, kdy nastavení analytického modelu, naplnění definovaných konstruktů může mít stejnou složitost jako

vývoj softwarového produktu a vyžaduje použití softwarových nástrojů. Vyžaduje taktéž jisté matematicko-statistické znalosti a schopnost analýzy. Proces měření je náročný na stabilní měřicí podmínky a schopnost měření provést opakovaně, tj. zajistit reliabilitu.

Otevřenou zůstává otázka vhodné **agregace měr** do jedné hodnoty a stanovení váhy jednotlivých měr v relaci. Zvolená lineární agregace a relativizované hodnoty mohou působit u vybraných měr poskytující celé nebo reálné hodnoty, možné je přemapovat ordinální míry na reálné, u výčtových hodnot však je nutné provést převod kvalitativně, resp. se takovým mírám vyhnout.

Aplikovaný postup pracoval s třídami opatření v kontextu části informačního systému (web rozhraní, emailový systém). Výběr tříd opatření T_O, které jsou do hodnocení zahrnuty je v tomto případě kvalitativní a zavádí do měření subjektivitu. Exaktní přístup stanovující konkrétní sadu opatření a nad ním stanovenou míru je schopen subjektivitu výrazně snížit.

V případových studiích byly použity vlastní experimentální detekční nástroje, nicméně existují komerční produkty, které podobnou úlohu plní obdobně. Bohužel tyto nástroje s výjimkou rozsáhlých enterprise řešení nejsou stavěny s úmyslem podporovat měření a neumožňují poskytovat statistiky a přímo je odesílat do zpracování.

Případové studie indikují ve zkoumaných oblastech očekávanou rozdílnou sílu relací „Vlastník cení informace“ a „Zpracovatel cení informace“. Indikuje jej sice nízká, nicméně stabilně opakovaná míra **email** a **web application leakage**. Rozdíl je v případě lidských zdrojů minimalizovatelný nasazením nástrojů, které vynucují provedení akce s vazbou na klasifikaci informace na straně zpracovatele.

7 ZÁVĚR

Rozvoj v oblasti zabezpečení informací v podmínkách českých orgaizací je charakterizován postupným rozšiřováním povědomí o hlavních faktorech ovlivňujících bezpečnost informací, kterými jsou dlouhodobě lidský faktor a kvalita technických prostředků ochrany. Tato skutečnost není nová, průběžné průzkumy stavu informační bezpečnosti opakovaně na tuto skutečnost dlouhodobě poukazují. Podle dalších výzkumů v ČR i v EU je požadavek zlepšování bezpečnosti informací prostřednictvím zabezpečování informačních systémů na třetím místě, následuje zlepšení služeb poskytovaných koncovým uživatelům a snížení nákladů na informační technologie. Roste dynamika prosazování požadavků na bezpečnost informací v legislativě a je stabilním tématem.

Disertační práce se zaměřila na kvantitativní hodnocení kritických charakteristik informací v podmínkách organizací v ČR. Měření podle provedeného výzkumu v ČR není považováno za hlavní faktor ovlivňující bezpečnost informací, zájem o tuto problematiku však v literaturních zdrojích nevykazuje pokles, neboť kvantifikace charakteristik a atributů určitých jevů a produktů je prostředkem pro zpřesňování a zdokonalování parametrů systému, resp. zvyšování účinnosti procesů.

Hlavním výstupem práce bylo stanovení metodiky pro hodnocení bezpečnosti informací v informačním systému. Bezpečnost informací jako produkt vyplývá z bezpečnostní pozice tohoto informačního systému v daném čase. Metodika vychází z identifikovaného modelu chování české organizace rozšířeného o proces měření podle ISO 27004. Rozšíření je voleno tak, aby zajistilo potřebný vliv výstupů měřicího procesu na proces zlepšování bezpečnosti informací v organizaci. Toho je dosaženo poskytnutím informací do zpětné vazby s možností ovlivnění modelu chování organizace směrem k riziku a minimalizace redukce výběrového souboru bezpečnostních opatření způsobené organizačními prioritami.

Pro naplnění hlavního cíle práce byl zvolen top-down přístup k identifikaci měr zaměřených na bezpečnost informací s využitím obecného konceptuálního nástroje Goal-Question-Metric autorem rozšířeného o verifikační fáze pro oblast bezpečnosti

informací. Identifikace pomocí nástroje GQM se ukázala jako netriviální a vyžaduje expertní teoretické znalosti z oboru. Pro usnadnění identifikace otázek a měr byla zavedena metoda verifikace výstupů kroků vývoje měr postavená na rozšířeném bezpečnostním modelu informace a na ochranných opatřeních definovaných vybraným standardem ISO 27004. Verifikace účinně zajišťuje uchování potřebných vazeb na rizika a na opatření.

Usnadněním pro organizace v praxi by byla možnost opakovaného použití identických měr (vybudování veřejného katalogu konstruktů měr) a případná následná možnost benchmarku mezi organizacemi.

Pro naplnění dílčích cílů práce byl realizován kvantitativní a kvalitativní výzkum, kdy byla zaměřena oblast zájmu případových studií v českých organizacích, která byla formulována jako „snížení vystavení informací zranitelnostem vycházejících z lidského faktoru“, „klasifikace informace“ a „odlišné vnímání rizik ve vztahu vlastník-informace a zpracovatel-informace“.

Pro realizaci měření podle navrženého modelu byl navržen a na konkrétní organizaci ověřen postup měření. Pomocí postupu byly iterativním přístupem vyvinuty tři míry, které jsou prezentovány v rámci praktické části práce jako případové studie. Výsledky měření realizovaného v dané organizaci jsou závislé především na použitém měřicím nástroji (specifický experimentální vývoj). Možnosti měřicího nástroje jsou omezené a sloužily pouze jako zdroj hodnot. Vhodnějším nástrojem by byly komerční produkty specializované na oblast prevence úniku dat (angl. DLP), které díky své zralosti zajišťují přesnější zdroj dat.

Kvantitativní výzkum byl proveden na reprezentativním vzorku organizací a výsledky lze zobecnit na výběrový soubor. Výzkum akceptoval **hypotézu 1**, že nejsou aplikovány postupy a standardy na bázi ISO standardů. Toto platí především pro malé a střední podniky. Z pohledu navrženého postupu by se mohlo zdát, že bude problém s aplikací konstruktů podle ISO 27004. To však není překážkou díky navrženému obecnému konstruktu GQM. Dále nebyla akceptována **hypotéza 2**, že organizace nestanovují priority při dosahování bezpečnosti informací. Priority jsou stanovovány. Naopak akceptována byla **hypotéza 3**, tj. že organizace nehodnotí informační systémy měřením. **Hypotéza 4** byla taktéž akceptována a potvrdilo se, že identifikované vlivné

faktory (lidský faktor a kvalita technických prostředků ochrany a další) považuje za důležité více než 50 % organizací.

Výzkumné otázky definované v cíli práce byly odpovězeny. Byla pozitivně zodpovězena **výzkumná otázka 1**, neboť navržené míry identifikované metodickým postupem přispívají k vyjádření bezpečnosti informací systémem navržených měr. Změřené hodnoty vypovídají o definované části informačního systému v podobě kvantitativně vyjádřené pozice tohoto systému. Bezpečnost informací jako produkt je přímo závislá na bezpečnostní pozici informačního systému. **Výzkumná otázka 2** byla odpovězena negativně. Konkrétní vyvinutá množina měr („Web application information leakage“ v organizaci A a „email application leakage“ v organizaci B) samostatně neposkytuje úplné (a tedy přesné) informace o úrovni bezpečnosti informací v celém systému. Ta je závislá na dalších relacích a entitách bezp. modelu, které s ohledem na aplikovanou redukci ochranných opatření v čase měření nebylo možné plně vyhodnotit. Řešením je pokrýt měřením celý informační systém a bezpečnostní pozici vyjádřit jako úplný výsledek agregace výstupů.

Použitý metodický postup za předpokladu pokrytí všech charakteristik informačního systému a zajištění kvalitativních parametrů měření a vhodné agregační funkce lze použít ke kvantitativnímu zhodnocení bezpečnosti informací. **Výzkumná otázka 3** byla odpovězena pozitivně, neboť na základě změn měřených hodnot v čase lze usuzovat na odchylky v chování měřených prvků informačního systému. Problematickým však zůstává mechanismus agregace a škály jednotlivých výstupů měření, který by měl být předmětem dalšího zkoumání.

Problémem při samotném procesu měření se ukazuje udržení kvalitativních charakteristik procesu měření, tj. spolehlivost (reliabilita), kontinuálnost a příprava vhodného měřicího nástroje. Tématy pro navazující práce je ochrana změřených hodnot ve smyslu integrity a důvěrnosti. S ohledem na skutečnost, že hodnoty vypovídají o pozici hodnoceného systému, mohou být cílem útočníků a jedná se tedy o citlivá data.

Na závěr je třeba říci, že práce se zaměřila na měření kritických charakteristik informací pokrývající vybranou část rozšířeného bezpečnostního modelu – entity „Vlastník“, „Zpracovatel“, „Informace“ a „Hodnota informace“ a vybrané relace mezi nimi. Vypovídají tedy přímo o těchto entitách a jejich charakteristikách. Obecně

diskutovanými oblastmi však mohou být i klíčové parametry souvisejících procesů (KPI) a sady odvozených charakteristik, které determinují např. „compliance“ a „conformance“, tj. soulady a konkrétními standardy a předpisy. Odvození těchto charakteristik je tématem pro případné navazující práce. Pokrytí dalších relací z bezpečnostního modelu je možné v dalších navazujících pracích, případně publikacích.

7. 1 Přínosy pro teorii

Vědecký přínos se předpokládá v odhalení závislostí mezi entitami na základě rozšířeného bezpečnostního modelu a na základě měření s využitím vytvořeného modelu chování organizace. Přínosem je i posílení významu abstraktního modelu Reference monitor jako základny pro hodnocení informačních systémů v různých podobách (počítačové systémy, lidé, manuální systémy).

Návazná výzkumná činnost může využít možnost kategorizace organizací podle modelového přístupu a směřovat k vytvoření konkrétního systému měr pro konkrétní přístup. Po kompletním ohodnocení a agregaci výstupů lze provést statickou vizualizaci bezpečnostní pozice informačního systému v organizaci na bázi změřených hodnot. Lze taktéž zapojit další oblast bezpečnosti informačních systémů (výpočetních a komunikačních systémů, spolehlivosti, pravděpodobnosti selhání a vzájemné závislosti) propojením s doménou kontinuity činnosti ICT.

7. 2 Přínosy pro praxi

Přínos pro praxi autor spatřuje v přehledu a analýze aktuálního stavu měření v oblasti informační bezpečnosti v České republice. Následné navržení postupu může být použito v iniciálních fázích zavádění ISO 27004 do praxe podniků, stejně po rozšíření a adaptaci jako realizaci povinností organizace vyplývajících z legislativních podmínek, konkrétně Zákona o kybernetické bezpečnosti. Metodika v podmínkách českých organizací přináší jednu z možných metod pro zpřístupnění procesů informační bezpečnosti veřejnosti. Poskytnuté výstupy umožňují zvýšení povědomí o oblasti řízení informačních rizik v dalších sektorech ekonomiky. Hlavní přínos je pak podpoření a zvýšení efektivnosti fáze ACT a auditní fáze CHECK v rámci procesů řízení

informační bezpečnosti na operativní úrovni a podporu rozhodování za jistoty o organizačních prioritách v oblasti bezpečnosti informací. Díky obecnosti lze metodiku po revizi ověřit v ostatních ekonomických sektorech.

Systematický vývoj měr navrženým postupem potenciálně umožňuje vývoj znovupoužitelného a do dalších organizací přenositelného systému měr, což zakládá možnost realizace moderního přístupu Security as a service. Vstupem do metodiky mohou být již existující kvantitativní metodiky, např. CVSS (Common Vulnerability Scoring System) a jiné.

8 POUŽITÁ LITERATURA

[1] ANDERSON, J. P.: *Computer Security Technology Planning Study*. Hanscom AFB, Bedford, MA, 1972. Technická zpráva ESDTR73-51.

[2] ANDERSON, R.: *Security Engineering*. USA: Wiley Publishing, 2008. ISBN 978-0-470-06852-6.

[3] ANDERSON, V.: *Research methods in human resource management*. London: Chartered Institute of Personnel and Development, 2009. ISBN 978-1-84398-227-2.

[4] BASILI, V.R., CALDIERA, C., ROMBACH H.D.: Goal Question Metric Paradigm. In *Encyclopedia of Software Engineering*. John Wiley & Sons, 1994. Volume 1, pp. 528-532.

[5] BROTBY, W., K.: *Information Security Management Metrics*. USA: Auerbach Publications, 2009. ISBN 978-1-4200-5285-5.

[6] BROTBY, W. K., HINSON, G.: *PRAGMATIC Security Metrics: Applying Metametrics to Information Security*. CRC Press, 2013. ISBN 9781439881538.

[7] ČECH, P., BUREŠ, V.: *Podniková informatika*. Hradec Králové: GAUDEAMUS, 2009. ISBN 978-80-7041-479-8.

[8] CHEW, E., SWANSON, M., STINE, K., BARTOL, N., BROWN, A., ROBINSON, W.: *NIST SP 800-55 Revision 1: Information security - Performance Measurement Guide for Information Security*. USA: National Institute Of Standards and Technology, 2008.

[9] ČSN ISO/IEC 2382-1 - Informační technologie - Slovník - Část 1: Základní termíny. Český normalizační institut, 1998.

[10] ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - systémy managementu bezpečnosti informací - Požadavky.

[11] ČSN ISO/IEC 27002:2008, Informační technologie – Soubor postupů pro management bezpečnosti informací.

[12] ČSN ISO/IEC TR 13335 – Informační technologie – Směrnice pro řízení bezpečnosti IT.

[13] DALER, T., GULBRANDSEN, R., MELGARD, B., SJOLSTAD, T.: *Security of information and data*. Ellis Horwood Limited, 1989. ISBN 0-7458-0575-2.

[14] DHILLON, G.: *Managing Information system security.* USA: Macmilian Press Ltd., 1997. ISBN 0-333-69260-8.

[15] DISMAN, M.: *Jak se vyrábí sociologická znalost*. Praha: Nakladatelství Karolinum, 2008. ISBN 978-80-246-0139-7.

[16] DOBDA, L.: *Ochrana dat v informačních systémech*. Praha: Grada Publishing, 1998. ISBN: 80-7169-479-7.

[17] DOSEDĚL, T.: *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[18] DOUCEK, P., NOVÁK, L., NEDOMOVÁ, L., SVATÁ, V.: *Řízení bezpečnosti informací. 2. vydání.* Praha: Professional publishings, 2011. ISBN 978-80-7431-050-8.

[19] DRUCKER, P. F.: *The comming of the new organisation. Harward business review on Knowledge management.* Harward Business Press, 1998. ISBN 978-087-584-8815.

[20] ERNST & YOUNG. *Czech Information Security Survey 2003*. Praha: DSM, Tate International s.r.o., 2003. ISBN 80-902858-8-0.

[21] GUTMANN, P.: *Cryptographic Security Architecture: Design and Verification.* New York: Springer Science & Business Media, 2004. ISBN 0-378-95387-6.

[22] HAYDEN, L.: *IT security metrics. A Practical framework for Measuring Security & Protecting Data*. USA: The McGraw-Hill Companies, 2010. ISBN 978-0-07-171340-5.

[23] HEBÁK, P. a kol.: *Vícerozměrné statistické metody 3*. Praha: Informatorium, 2005, ISBN 80-7444-049-4.

[24] Heinzle, B., Furnell, S., M.: Assessing the Feasibility of Security Metrics. In *Proceedings to 10th International Conference Trustbus.* Praha, 2013. Volume 8058 2013, pp. 88-95. ISBN: 978-3-642-40342-2.

[25] HENDL, J.: *Přehled statistických metod zpracování dat.* Praha: Portál, 2006. ISBN 80-7467-124-9.

[26] HENDL, J.: *Kvalitativní výzkum. Základní teorie, metody a aplikace.* 3. vydání. Praha: Portál, s. r. o., 2012, ISBN 978-80-262-0219-6.

[27] HERRMANN, D., S.: *Complete Guide to Security and Privacy Metrics.* USA: Auerbach Publications, 2007. ISBN 978-0-8493-5402-1.

[28] HÖNIGOVÁ, A., MATYÁŠ, V.: *Anglicko–česká terminologie bezpečnosti informačních technologií.* 1. vydání. Praha: Computer Press, 1996. ISBN 80-85896-44-3.

[29] ISACA: *COBIT 5: Enabling information*. Rolling Meadows: ISACA, 2013. ISBN 978-1-60420-349-3.

[30] ISO/IEC 17799:2006 Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací.

[31] ISO/IEC 21827 Technology - Systems Security Engineering - Capability Maturity Model.

[32] ISO/IEC 27004:2009 – Information technology – Security techniques – Information security management measurements.

[33] ISO/IEC 27005:2008 – Information technology – Security techniques – Information security risk management.

[34] ISO/IEC 27006:2007 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management system.

[35] JAQUITH, A.: *Security Metrics. Repacing Fear, Uncertainty, and Doubt.* USA: Pearson Education Inc., 2009. ISBN 978-0-32-134998-9.

[36] JOUINI, M., RABAI, L. B. A., AISSA, A. B.: Classification of Security Threats in Information Systems. In *Proceedings to The 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), the 4th International Conference on Sustainable Energy Information Technology (SEIT-2014).* Procedia Computer Science, 2014. Volume 32, pp. 489–496.

[37] KOUNS, J., MINOLI, D.: *Information Technology Risk Management in Enterprise Environments*. USA: Wiley Publishing, 2010. ISBN 978-0-471-76254-6.

[38] KRIŠTOUFEK, K.: *Oborová encyklopedie.* Výpočetní a řídící technika. Praha: SNTL, 372 s., 1986.

[39] Kritéria hodnocení zabezpečených počítačových systémů: *Trusted Computer System Evaluation Criteria*. Praha: BEN - Technická literatura, 1994.

[40] LANDOLL, D., J.: *The Security Risk Assessment Handbook*. USA: Auerbach Publications, 2006. ISBN 978-0-8493-2998-2.

[41] MERNA, T., AL-THANI, F. F.: *Risk management, řízení rizik ve firmě*. Brno: Computer Press, a. s., 2007. ISBN 978-80-2511547-3.

[42] OUEDRAOGO, M., KHADRAOUI, D., MOURATIDIS, H., DUBOIS, E.: *Appraisal and reporting of security assurance at operational systems level.* USA: Elsevier Science Inc. New York, 2012. In *Journal of Systems and Software* 01/2012. p.p.:193-208. ISSN 0164-1212.

[43] PELTIER, R. T.: *Information Security Policies, Procedures, and Standards.* USA: Auerbach publications, 2002. ISBN 0-8493-1137-3.

[44] POŽÁR, J.: *Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s. r. o., 2005. ISBN 80-86898-38-5.

[45] ŘEZANKOVÁ, H.: *Analýza dat z dotazníkových šetření.* PBtisk Příbram, 2007, ISBN 978-80-86946-49-8.

[46] SAVOLA, R.: Towards a taxonomy for information security metrics. In *Proceedings of the 2007 ACM workshop on Quality of protection*, 2007. ACM, New York and NY and USA, pp. 28–30.

[47] SAVOLA, R.: *On the feasibility of utilizing security metrics in software-intensive systems*. 2010. IJCSNS International Journal of Computer Science and Network Security 10(1).

[48] SKALKOVÁ, J. a kol.: *Úvod do metodologie a metod pedagogického výzkumu*. 2. vydání. Praha: SPN, 209 s., 1983.

[49] SMEJKAL, V., RAIS, K.: *Řízení rizik ve firmách a jiných organizacích.* 2. vydání. Praha: Grada Publishing, 2006. ISBN 80-247-1667-4.

[50] SOLINGEN, V., R., BERGHOUT, E.: *The Goal/Question/Metric Method: a practical guide for quality improvementof software development*. London: McGraw-Hill Publishing Company, 1999. ISBN 9780077095536

[51] SOLMS, B., V.: Information Security – The Fourth Wave. In *Proceedings from Conference Computers & Security*, 2006. Vol. 25, pp.165-168. ISSN 0167-4048.

[52] STEVENSON, W. J.: *Introduction to Management Science*. Homewood: IRWIN, 1989. ISBN: 0-256-03660-8.

[53] TILBORG, VAN, H., JAJODIA, S.: *Encyclopedia of Cryptography and Security*. Londýn: Springer Science+Business Media, 2011. ISBN 978-1-4419-5905-8.

[54] UČEŇ, P.: *Metriky v informatice.* Praha: Grada Publishing, 2001. ISBN 80-247-0080-8.

[55] VANÍČEK, J.: *Měření a hodnocení jakosti informačních systémů.* Praha: ČZU v Praze, 2004. ISBN 80-213-1206-8.

[56] VEBER, J. a kol.: *Management: Základy - prosperita - globalizace.* Praha: Management Press, 2000. ISBN 80-7261-029-5.

[57] WHITMAN, M., MATTORD, H.: *Management of Information Security*. USA: Course Technology, Cengag Learning, 2010. ISBN 0-8400-3160-2.

[58] Zákon č. 101/2000 Sb., Zákon o ochraně osobních údajů a o změně některých zákonů.

[59] Zákon č. 106/1999 Sb., Zákon o svobodném přístupu k informacím.

[60] Zákon č. 240/2000 Sb., Zákon o krizovém řízení a o změně některých zákonů.

[61] Zákon č. 365/2000 Sb. o informačních systémech veřejné správy, navazující vyhlášky.

[62] Zákon č. 412/2005 Sb., Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Internetové zdroje:

[63] CCRA: *Common Criteria for Information Technology Security Evaluation.* CCRA, 2012.
Dostupný z:
https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf
https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf

https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf
[Citováno: 25.4.2015]

[64] ČZU: *Bezpečnostní řád. Bezpečnostní politika informací.* Praha: ČZU, 2008. Dostupný z:
<http://katedry.czu.cz/storage/3049_Verejne_bezpecnostni_politika_informaci.pdf>
[Citováno: 7.4.2015].

[65] DOD: *Trusted Computer System Evaluation Criteria*. USA: Department of Deffense, 1985. Dostupný z: http://csrc.nist.gov/publications/history/dod85.pdf
[Citováno: 25.4.2015]

[66] DOTAI: *Information Technology Security Evaluation Criteria (ITSEC).* Francie: Department of Trade and Industry, 1991. Dostupný z:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile
[Citováno: 25.4.2015]

[67] ENISA: *What does ENISA do?*. Řecko: European agency for Network and Information Security, 2015.
Dostupný z: < https://www.enisa.europa.eu/about-enisa/activities>
[Citováno: 7.6.2015]

[68] HANÁČEK, P., STAUDEK, J.: *Bezpečnost informačních systémů: Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha: Úřad pro státní informační systém, 2000. Dostupný z: <http://www.micr.cz/files/479/uvis-Bezpecnost-20000701.pdf>. [Citováno: 15.6.2013]

[69] JANSEN, W. A.: *Directions in security metrics research*. Gaithersburg: National Institute of Standards and Technology, 2009. Dostupný z: <http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf>
[Citováno 25 Dec 2011]

[70] MERRIAM-WEBSTER. *Security. Safety*. Merriam-Webster. Dostupný z: <www.m-w.com/cgi-bin/dictionary>.
[Citováno: 12. 1. 2013]

[71] NATALE, D.: *Complexity and data quality*. Researchgate, 2015. Dostupný z: <http://www.researchgate.net/publication/265796772_Complexity_and_data_quality>
[Citováno: 17. 6. 2015]

[72] CHEW, E., SWANSON, M., STINE, K., BARTOL, N., BROWN, A., ROBINSON, W.: *Security Metrics Guide for Information Technology Systems*. NIST Special Publication 800-55, 1. revize, July 2008. Dostupný z: < http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf >
[Citováno: 13. 6. 2014]

9 SEZNAMY

9. 1 Seznam grafů

9. 2 Seznam schémat

9. 3 Seznam tabulek

10 PŘÍLOHY

10. 1 Struktura dotazníkového šetření

Katedra informačního inženýrství

DOTAZNÍK

Vážená paní, Vážený pane,

dovoluji se na Vás jako zástupce vybrané organizace obrátit s prosbou o vyplnění dotazníku zaměřeného na hodnocení bezpečnosti informací v informačních systémech. V rámci zpracování disertační práce s názvem „Hodnocení bezpečnosti informací v informačních systémech“ na Katedře informačního inženýrství Provozně ekonomické fakulty České zemědělské univerzity v Praze, realizuji výzkum v organizacích v České republice. Statisticky vyhodnocený dotazník se stane podkladem pro zpracování disertační práce a pro publikování vědeckých článků.

Vyplnění dotazníku v aplikaci LimeSurvey trvá přibližně 10-15 minut. Prosím postupujte podle instrukcí u jednotlivých otázek (pokud není uvedeno jinak, zaznačte jednu odpověď). Dotazník prosím vyplňte a odešlete do 14 dní od jeho obdržení. Vyplnění dotazníku je anonymní.

Předem Vám děkuji za Vaši ochotu a spolupráci.

Jiří Urbanec

OTÁZKY:

1. Ve vaší organizaci zpracováváte obchodní, účetní, zákaznické nebo jiné informace v informačních systémech (informační systém zahrnuje personál, technické a funkční prostředky):
   a. ☐ výhradně manuální (kartotéka, písemné dokumenty, rukou psané poznámky, telefonické hovory, poštovní zásilky, apod.),
   b. ☐ většinou manuálních, z méně než 30 % počítačových,
   c. ☐ většinou počítačových, z méně než 30 % manuálních,
   d. ☐ výhradně počítačových, manuálních z méně než 10 %,
   e. ☐ nevím.
2. Zpracováváte hodnotné informace, jejichž ztráta nebo vyzrazení by znamenala škodu pro vaši organizaci nebo jiné subjekty (osobní údaje, údaje klientů, obchodní tajemství apod.)?
   a. ☐ ano,
   b. ☐ ne,
   c. ☐ nemáme zjištěno, ale pravděpodobně ano,
   d. ☐ nemáme zjištěno, ale pravděpodobně ne,
   e. ☐ jiné (prosím uveďte)……,
   f. ☐ nevím.
3. Informační systémy z pohledu rizika pro hodnotné informace:
   a. ☐ hodnotíme,
   b. ☐ nehodnotíme.

3a. Pokud informační systém nehodnotíte, co je důvodem?
   a. ☐ Nepovažujeme to za důležité.
   b. ☐ Předpokládáme, že informační systém je bezpečný.
   c. ☐ Neexistují postupy pro hodnocení, resp. nevíme co hodnotit.
   d. ☐ Postupy pro hodnocení jsou finančně či jinak náročné.
   e. ☐ Jiné (prosím uveďte)…….

3b. Pokud informační systém hodnotíte, cílem hodnocení je (lze označit více odpovědí):
   a. ☐ porozumění bezpečnostním rizikům,
   b. ☐ identifikace vznikajících problémů a slabin,
   c. ☐ potvrzení účinnosti nastavených protiopatření,
   d. ☐ zlepšování procesů informační bezpečnosti,
   e. ☐ jiné (prosím uveďte)……

4. Měření bezpečnosti informací v informačním systému, případně jiný kvantitativní způsob hodnocení informačního systému, ve vaší organizaci:
   a. ☐ je aplikován,
   b. ☐ není aplikován,
   c. ☐ nevím.

4a. Pokud je aplikováno měření příp. kvantitativní hodnocení informačního systému, pak využíváte:
   a. ☐ monitoring součástí informačního systému a sledování četností příp. trendů,
   b. ☐ měření konkrétních přesně stanovených charakteristik informačního systému a jejich analýzu vhodnými matematicko-statistickými metodami,
   c. ☐ jiný způsob (prosím uveďte)……

5. Prosím ohodnoťte důležitost vašich organizačních cílů při dosahování bezpečnosti informací (1= zcela nedůležitá, 5= velmi důležitá, lze přiřadit stejnou důležitost):
   ☐ ekonomické (finanční) (zachování ekonomické optimálnosti a návratnosti),
   ☐ personální (zajištění bezpečnosti informací personálními opatřeními),
   ☐ technické (zajištění bezpečnosti informací fyzickými a technickými opatřeními),
   ☐ legislativní (dosažení souladu s legislativou)

6. Označte faktory, které mají ve vaší organizaci hlavní vliv na dosažení maximální úrovně bezpečnosti informací (lze označit více odpovědí):
   a. ☐ identifikace rizik působících na konkrétní informační aktiva,
   b. ☐ prostředky ochrany důvěrnosti, integrity a dostupnosti informací,
   c. ☐ klasifikace informací,
   d. ☐ lidský faktor,
   e. ☐ kvalita procesů řízení informační bezpečnosti a prosazování bezpečnostní politiky,
   f. ☐ monitoring osob, technických prostředků a informačních procesů,
   g. ☐ měření bezpečnostních charakteristik informačního systému,
   h. ☐ jiné (prosím uveďte) ……..

7. Podle které normy řešící systém řízení informační bezpečnosti se řídí vaše organizace (lze označit více odpovědí):
   a. ☐ ISO rodiny 27000,
   b. ☐ ISO 17799 (ČSN ISO 17799),
   c. ☐ ISO 13335 (ČSN ISO 13335),
   d. ☐ BS 7799 (ČSN BS 7799),
   e. ☐ NIST SP-800,
   f. ☐ COBIT,
   g. ☐ ITIL,
   h. ☐ zákonné normy,
   i. ☐ vlastní interní směrnice a standardy nezávislé na výše uvedených,
   j. ☐ žádné,
   k. ☐ jiné (prosím uveďte) ……..
   l. ☐ nevím.

8. Celkovou bezpečnost informací v organizaci, ve které pracujete, řeší pozice:
   a. ☐ specialista na nemanažerské pozici,
   b. ☐ manažer IT,
   c. ☐ manažer na úrovni divize/útvaru/odboru,
   d. ☐ rada pro obecnou bezpečnost a bezpečnost IT,
   e. ☐ nejvyšší vedení,
   f. ☐ žádná,
   g. ☐ jiná (prosím uveďte) .....

IDENTIFIKAČNÍ OTÁZKY:

Ve kterém odvětví působí vaše organizace (podle hlavního předmětu činnosti)? (Sekce jsou uvedeny dle Klasifikace ekonomických činnosti – CZ-NACE)

   a. ☐ zemědělství, lesnictví a rybářství,
   b. ☐ těžba a dobývání,
   c. ☐ zpracovatelský průmysl,
   d. ☐ výroba a rozvod elektřiny, plynu, tepla,
   e. ☐ zásobování vodou, činnosti související s odpady,
   f. ☐ stavebnictví,
   g. ☐ velkoobchod a maloobchod, oprava motorových vozidel,
   h. ☐ doprava a skladování,
   i. ☐ ubytování, stravování a pohostinství,
   j. ☐ informační a komunikační činnosti, poradenské činnosti,
   k. ☐ peněžnictví a pojišťovnictví,
   l. ☐ činnosti v oblasti nemovitostí,
   m. ☐ profesní, vědecké, technické činnosti,
   n. ☐ administrativní a podpůrné činnosti,
   o. ☐ veřejná správa a obrana, povinné sociální zabezpečení,
   p. ☐ vzdělávání a výzkum,
   q. ☐ zdravotní a sociální péče,
   r. ☐ kulturní, zábavní a rekreační činnosti,
   s. ☐ ostatní činnosti (prosím uveďte): .....

Velikost organizace:

   a. ☐ do 50 zaměstnanců,
   b. ☐ 51 až 249 zaměstnanců,
   c. ☐ 250 a více zaměstnanců.

Organizace, ve které pracujete, je z hlediska většinového vlastnického podílu:

   a. ☐ českou organizací,
   b. ☐ zahraniční organizací.

Organizace, ve které pracujete, využívá outsourcing pro:

a. ☐ internetové připojení,
b. ☐ správu antivirů/firewallů,
c. ☐ vývoj aplikací,
d. ☐ správu databází,
e. ☐ správu lokální sítě nebo správu WAN,
f. ☐ provoz a údržbu informačních systémů,
g. ☐ finanční nebo účetní systém,
h. ☐ bezpečnostní monitoring,
i. ☐ jiný (prosím uveďte).....

Jakou pozici v organizaci zastáváte?

a. ☐ ředitel, jednatel nebo majitel společnosti,
b. ☐ obchodní, technický nebo provozní ředitel,
c. ☐ ekonomický nebo finanční ředitel,
d. ☐ vedoucí oddělení,
e. ☐ technik/specialista/řadový zaměstnanec,
f. ☐ ředitel informačních systémů / informačních technologií,
g. ☐ vedoucí oddělení informačních systémů / informačních technologií,
h. ☐ specialista informačních systémů / informačních technologií,
i. ☐ manažer bezpečnosti informačních systémů / informačních technologií,
j. ☐ specialista bezpečnosti informačních systémů / informačních technologií,
k. ☐ jiná (prosím uveďte).....

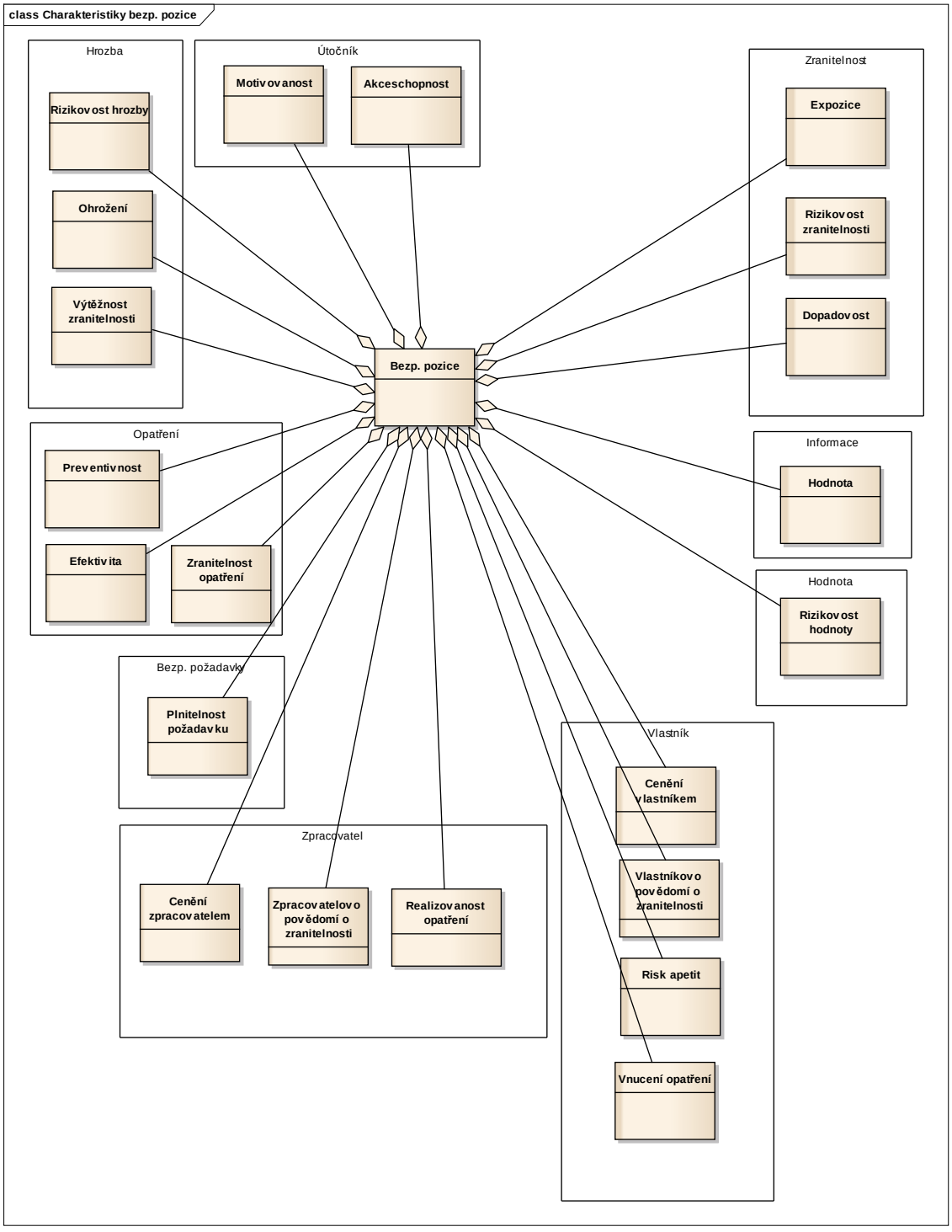
Ještě jednou Vám děkuji za ochotu a čas, který jste vyplnění tohoto dotazníku věnoval(a). Máte-li otázky k tématu či připomínky, prosím, kontaktujte mě na emailu urbanec@pef.czu.cz.

10. 2 Struktura rozhovorů

Skup.	Otázka
Informační aktiva	Pracujete s vlastními riziky, odlišujete se od jiných organizací v sektoru pokud se týká zpracovávaných dat?
	Vyplývají hlavní informační rizika (rizika pro informace) z organizační struktury, z assetů nebo ze struktury IS? Existuje mezi některými přímá vazba?
	Existuje reuse assetů nebo IS? V jaké formě?
	Na základě bezpečnostního modelu: kterou z jeho entit aplikujete jako komoditu ? Rozšířili byste tento model o nějakou součást? Jaká je vaše organizační struktura? Která role řeší informační bezpečnost? Komu podléhá CISO?
	Kdybyste měl/měla pochválit, nebo zkritizovat, s ohledem na postupy a opatření vyplývající z vámi aplikované normy: přistupuje organizace k řešení informační bezpečnosti komplexně do hloubky, nebo redukuje (vědomě, nevědomě) ochranná opatření (jak mnoho? nevíme/vůbec/málo/hodně, rovnoměrně/různě přes organizaci).
	Jakým způsobem identifikujete zranitelnosti, hrozby? Systematickým postupem/programem, adhoc náhodně. Jak je to s riziky v oblasti lidských zdrojů? Na jaké úrovni je povědomí o bezpečnosti informací mezi zaměstnanci, nebo zaměstnanci spoléhají na bezpečnost IS a okolí?
	Máte stanovenu obchodní (případně jinou) hodnotu informací, které jsou u vás zpracovávány? Pokud nejste primární poskytovatel ale součást dodavatelského řetězce, jak chráníte informace vašich partnerů? Považujete se za důležitou součást článku?
Zralost procesů informační bezpečnosti	Jakým způsobem stanovujete kvalitu bezpečnostního projektu, resp. požadavky na technické řešení při tvorbě systému? Jak dosažení těchto parametrů ověřujete? Jak totéž řešíte za provozu?
	Pokud používáte monitoring, na které oblasti se zaměřuje a jak je dosaženo kvality monitoringu (pokrytí, relevance, kontinuita, validita)
	Který údaj nejspolehlivěji vypovídá o vzniku útoku a dopadu bezpečnostního incidentu, resp. o datech (zda byla kompromitována)?
	Jakým způsobem detekujete kompromitaci dat? Budete schopni kompromitaci dat identifikovat a stanovit dopad v konkrétním případě? Jste schopni poskytnout důkaz „kompromitace“ nebo „nekompromitace“ konkrétních informací?
	Jakým způsobem reagujete na změnu bezpečnostní pozice systému a jak je tato doba dlouhá (minuty, vteřiny, hodiny, dny, týdny, měsíce).
	Jaký je vliv bezpečnostních opatření na user experience? Negativní, neutrální, pozitivní? Existují nějaké omezující podmínky?
	Máte definovanou enteprise architekturu, jste schopni stanovit hranice systému, vlastníka, organizace? Má toto efekt?
	Můžete konkrétnímu systému věřit a je prostor pro zlepšování? Jak reagujete na nové technologie?
Měření	Reflektuje kvalita procesů informační bezpečnosti úroveň dosažené bezpečnosti informací? Není rozpor s počtem data breaches?
	Na úrovni top managementu, jaké míry jsou vhodné, přijatelné, přípustné?
	Které typy charakteristiky jste schopni na úrovni IS měřit?
	Které charakteristiky jste schopni zpracovat a vyhodnotit?
	Jaké nástroje a schopnosti máte k dispozici při analýze změřených údajů?
	Jakým postupem stanovujete míry, referenční hodnoty apod? Jakým způsobem stanovujete oblasti měření?
	Na jaké problémy narážíte při stanovování metrik? Narážíte na konkrétní problémy při měření?

10. 3 Charakteristiky určené pro měření

Hodnotitelné charakteristiky bezpečnostní pozice informačního systému



Zdroj: vlastní zpracování

10. 4 Šablona konstruktu míry pro GQM model

<Unikátní organizační identifikátor bezpečnostního cíle>	
Specifikace cíle (Gk)	Cíl měření by měl být definován srozumitelně a měl by být jasně strukturovány. Měl by být na základě analýzy definován účel (předmět měření a proč), hledisko (za jakých aspektů a kdo) a charakteristika kontextu. Cíl by měl být relevantní pro účely zajištění bezpečnosti informací, reprezentovat strategické cíle vedení organizace a podporovat procesy s velkou prioritou. Vedení by mělo být schopno ukázat, jak cíle měření souvisí s bezpečnostními cíli a podporují zvyšování bezpečnosti informací. Cíl je definován na abstraktní úrovni.
Zájmové skupiny	Výčet konkrétních rolí, resp. subjektů, které závisejí resp. spoléhají na výsledky měření, účastní se zadání cíle a jeho vyhodnocení.
Definice cílové oblasti bezpečnostního modelu a souvisejících entit.	Výčet entit rozšířeného bezpečnostního modelu, které jsou předmětem zájmu. Specifikace entit podporuje relevantnost cíle v oblasti bezpečnosti infornací. Přiměřený počet entit je 2-4. Pokud nelze žádnou entitu namapovat, nejedná o cíl relevantní k bezpečnosti informací. Uvedení obslati verifikuje relevantnost cíle.
Specifikace otázek [1..m]	
Otázka (Gk-Qm)	Otázky jsou zpřesněním cíle na operativní úrovni. Odpovědí na otázky by mělo být možno vytvořit uspokojivý závěr, zda cíl byl splněn.
Očekávaná odpověď (Qm)	Očekávaná odpověď je formulována jako hypotéza. Odpověď může sloužit pro nastavení rozsahů pro indikátory.
Množina vazeb mezi entitami rozšířeného bezpečnostního modelu	Výčet entit a vazeb, které jsou předmětem měření. Otázka by se měla vázat na konkrétní entitu, resp. její konkrétní atribut.
Množina tříd protiopatření standardu ISO 27002:2009	Výčet výběrových opatření, která ovlivňují vazbu mezi sledovanými entitami. Pro každou identifikovanou vazbu/entitu by měla být identifikována neprázdná výběrová množina tříd opatření.
Specifikace měr [1..n]	
Míra (Gk-Qm-Mn) <název>	Míra poskytuje kvantitativní informace pro uspokojivé zodpovězení otázky. Míra je zpřesnění otázky do kvantifikace procesu nebo produktu. Po zjištění všech měr by měly být k dispozici všechny informace pro zodpovězení otázky. Vlivné faktory měření by taktéž měly být zhodnoceny a zahrnuty v definici míry, nebo určeny jako samostatné míry.
Atributy	Výčet měřitelných atributů předmětu měření.
Základní míry	Výčet základních měr a technik sběru dat.
Metoda měření	Výčet technik sběru dat. Souhrnný výčet, přesný způsob měření je uveden v měřicím konstruktu podle vybraného standardu. Pokud měření vyžaduje speciální nástroj nebo sondu, jsou zde uvedeny základní parametry tohoto nástroje s odkazem na design nástroje.
Odvozená míra a měřicí funkce	Výčet odvozených měr a měřicích funkcí
Indikátor a analytický model	Specifikace indikátoru a analytického modelu. Detail indikátoru je uveden v konkrétním konstruktu míry.
Zhodnocení míry	Sumarizuje výsledek procesu verifikace akceptovatelnosti míry
Metoda hodnocení míry, hodnotitelé a kritéria pro akceptaci míry.	Specifikuje způsob zhodnocení akceptovatelnosti míry (kvalitativně, PRAGMATIC (Brotby, 2012), jiné) a jmenovitý seznam hodnotitelů a jejich rolí (klient, oponent, vlastník předmětu měření). V případě metody PRAGMATIC probíhá hodnocení bodovací metodou anonymně pro všechna vybraná kritéria. Agregace je

	provedena aritmetickým průměrem a výsledné relativní skóre je vypočteno jako aritmetický průměr hodnocení jednotlivých kritérií jednotlivými hodnotiteli.
Skóre míry	Viz Skórovací karta PRAGMATIC. Kritérium pro akceptaci míry: *Avg(All) > 80%*
Výsledek akceptace míry	AKCEPTOVÁNA/NEAKCEPTOVÁNA podle kritéria pro akceptaci míry

Zdroj: vlastní zpracování dle Solingen etal (1999) a Brotby (2012)

Vzor skórovací karty PRAGMATIC

Hodnotitel	**P**	**R**	**A_1**	**G**	**M**	**A_2**	**T**	**I**	**C**	**All**
										%
	Avg(P)	Avg(R)	Avg(A_1)	Avg(G)	Avg(M)	Avg(A_2)	Avg(T)	Avg(I)	Avg(C)	Avg(All)

Zdroj: vlastní zpracování dle Solingen etal (1999) a Brotby (2012)

10. 5 Šablona konstruktu míry podle ISO 27004:2009

<Identifikace měřicího konstruktu>	
Měřicí konstrukt	**Název měření**
Identifikátor	Unikátní, organizačně specifický numerický identifikátor
Účel měřicího konstruktu	Popisuje důvod pro zavedení měřicího konstruktu
Cíl měření opatření/procesní	Cíl měření opatření/procesní (plánovaný nebo implementovaný).
Opatření (1)/Proces (1)	Měřené opatření/proces
Opatření (2)/Proces (2)	Volitelné: další opatření/procesy v seskupení zahrnuté ve stejné míře (plánované nebo implementované).
Předmět měření a atributy	
Předmět měření	Předmět (entita), která je charakterizována měřením jeho atributů. Předmět může zahrnovat procesy, plány, projekty, zdroje a systémy, nebo systémové komponenty.
Atribut	Vlastnost nebo charakteristika předmětu měření, která může být rozlišena kvantitativně nebo kvalitativně lidskými nebo automatizovanými prostředky.
Specifikace základních měr (pro každou základní míru [1...n])	
Základní míra	Základní míra je definována popisem atributu a specifikované měřicí metody pro její kvantifikaci (např. počet vyškolených osob, aktuální kumulativní cena). Hodnota je základní míře přiřazována během sběru dat.
Metoda měření	Logický sled operací použitých při kvantifikaci atributu s ohledem na definovaný rozsah.
Typ měřicí metody	V závislosti na povaze operací použitých při kvantifikaci atributu jsou rozlišovány dvě metody: -Subjektivní: kvantifikace zapojuje lidský úsudek -Objektivní: kvantifikace je založena na numerických principech (např. četnosti).
Škála	Seřazená množina hodnot nebo kategorií na které je atribut základní míry mapován.
Typ škály	V závislosti na povaze vztahu mezi hodnotami škály jsou definovány čtyři běžné typy: nominální, ordinální, intervalové a poměrné.
Jednotka měření	Konkrétní množství, definované a přijatelné, se kterou může být jiné množství porovnáno k vyjádření poměru dvou kvantit jako číslo.
Specifikace odvozených měr	
Odvozená míra	Míra, která je odvozena jako funkce dvou základních měr.
Měřicí funkce	Algortmus nebo výpočet pro kombinaci dvou nebo více základních měr. Škála a jednotka odvozené míry závisejí na škálách a jednotkách základních měr, ze kterých je složena, a taktéž na způsobu, jakým jsou kombinovány měřicí funkcí.

Specifikace indikátoru	
Indikátor	Míra, která poskytuje odhad nebo vyhodnocení specifických atributů odvozených z analytického modelu s ohledem na definovanou informační potřebu. Indikátory jsou základnou pro analýzu a rozhodování.
Analytický model	Algoritmus nebo výpočet kombinující jednu nebo více základních nebo odvozených měr s asociovanými rozhodovacími kritérii. Je založen na znalosti nebo předpokladech nebo vztazích základních nebo odvozených měr nebo chování v čase. Analytický model produkuje odhady nebo výpočty podstatné pro definovanou informační potřebu.
Specifikace rozhodných kritérií	
Rozhodné kritérium	Hranice, cíle nebo vzory použité k určení potřeby reagovat nebo další analýzy, nebo k popipsu úrovně jistoty k danému výsledku. Rozhodná kritéria pomáhají interpretovat výsledky měření.
Výsledky měření	
Interpretace indikátoru	Popis jak by vzorek indikátoru měl být interpretován.
Formát hlášení	Měl by být identifikován a dokumentován formát hlášení výstupů. Formát popisuje, které pozorování chce organizace nebo vlastník informace zaznamenat. Formát hlášení vizuálně znázorní míry a poskytne slovní vysvětlení indikátorů. Formát hlášení by měl být přizpůsoben pro účely příjemce informace.
Zájmové skupiny	
Klient pro měření	Řídící orgán nebo jiné zapojené skupiny požadující nebo závisející na informaci o efektivitě systému řízení informační bezpečnosti, opatření nebo skupiny opatření.
Oponent měření	Osoba nebo organizační jednotka, která validuje, že vyvinuté měřicí konstrukty jsou patřičné k hodnocení efektivity systému řízení, opatření nebo skupiny opatření.
Vlastník informace	Osoba nebo organizační jednotka, která vlastní informaci o předmětu měření a atributech a je odpovědná za měření.
Sběratel informace	Osoba nebo organizační jednotka odpovědná za sběr, zaznamenání a ukládání dat.
Zprostředkovatel informace	Osoba nebo organizační jednotka odpovědná za analýzu dat a zprostředkování výsledné informace.
Frekvence/Perioda	
Frekvence sběru dat	Určení, jak často jsou data sbírány.
Frekvence datové analýzy	Určení, jak často jsou data analyzovány.
Frekvence hlášení měřených výsledků	Určení, jak často jsou výsledky měření hlášeny (může být méně často než měření).
Revize měření	Datum revize měření (vypršení nebo obnova validity měření).
Perioda měření	Určení periody měření.

Zdroj: přeloženo autorem podle ISO 2004 (2009)

10. 6 Konstrukt míry GQM, Organizace A, G1

A_APP1_INFOSEC_G1	
Specifikace cíle (G1)	Dlouhodobě identifikovat všechny vlastníkem (E3) klasifikované (E2) informace (E1), které jsou zpracovávány, ukládány a přenášeny (E4) v rámci inhouse vyvíjených webových aplikací neidentifikovaným/neautorizovaným zpracovatelem/útočníkem (E4).
Zájmové skupiny	Odbor provozu a vývoje IT, Chief Information Security Officer, Obchodní vlastník aplikace
Definice cílové oblasti bezpečnostního modelu a souvisejících entit.	E1 – Informace E2 – Hodnota informace E3 – Vlastník informace E4 – Zpracovatel informace
Specifikace otázek	
Otázka (G1-Q1)	Kolik informací je v konkrétní aplikaci zpracováváno v rozporu s přístupovými oprávněními definovanými vlastníkem.
Očekávaná odpověď (Q1)	V aplikaci InternetBanking je zpracováváno maximálně 2% informací v rozporu s přístupovými oprávněními definovanými vlastníkem.
Množina vazeb mezi entitami rozšířeného bezpečnostního modelu	E4 - E1 (Zpracovatel cení informace)
Množina tříd protiopatření standardu ISO 27002:2009	Sekce 8: Správa informačních aktiv, 8.1, 8.2. Třída opatření pro určení vlivu na C, I, A: RIZ_PRISTUPU.
Specifikace měr	
Míra (G1-Q1-M1)	Relativní množství datových elementů webové aplikace, které na frontend úrovni jsou zpracovány a zobrazovány bez aplikace správných přístupových oprávnění ve všech případech užití.
Atribut (a1)	Počet zapsaných objektů (elementů datového modelu) v Reference Monitoru
Atribut (a2)	Počet čtených objektů (elementů datového modelu) z Reference Monitoru
Atribut (a3)	Počet známých subjektů přistupujících na Reference monitor
Atribut (a4)	Počet otestovaných případů užití aplikace
Atribut (a5)	Počet případů užití aplikace
Základní míra (m1)	Počet datových elementů z datového modelu aplikace, které jsou přenášeny na klientskou stanici.
Metoda měření (m1)	Diferenciální analýza TCB vs. webová aplikace metodou Reference monitoru, viz Design nástroje WAR-RMO.
Základní míra (m2)	Počet datových elementů z datového modelu aplikace (včetně vývojových), které nemají přiřazenu klasifikaci a zpracovávány na klientské stanici a přenášeny na ni.
Metoda měření (m2)	Diferenciální analýza TCB vs. webová aplikace metodou Reference monitoru, viz Design nástroje WAR-RMO.
Odvozená míra a měřicí funkce	$\mu_{G1_{Q1}} = \frac{m2}{m1}$
Indikátor a analytický model	Web application information classification coverage, G1-Q1-M1 > 98%
Zhodnocení míry	
Metoda hodnocení míry, hodnotitelé a kritéria pro akceptaci míry.	PRAGMATIC, 3 hodnotitelé, jména na žádost neuvedena H1 - IT specialista H2 - Security Architect

	H3 - obchodní vlastník aplikace Kritérium pro akceptaci míry: *Avg(All) > 80%*
Skóre míry	Viz skórovací karta PRAGMATIC
Výsledek akceptace míry	AKCEPTOVÁNA podle kritéria pro akceptaci míry, **Skóre = 85,70%**

Zdroj: vlastní zpracování

Skórovací karta PRAGMATIC

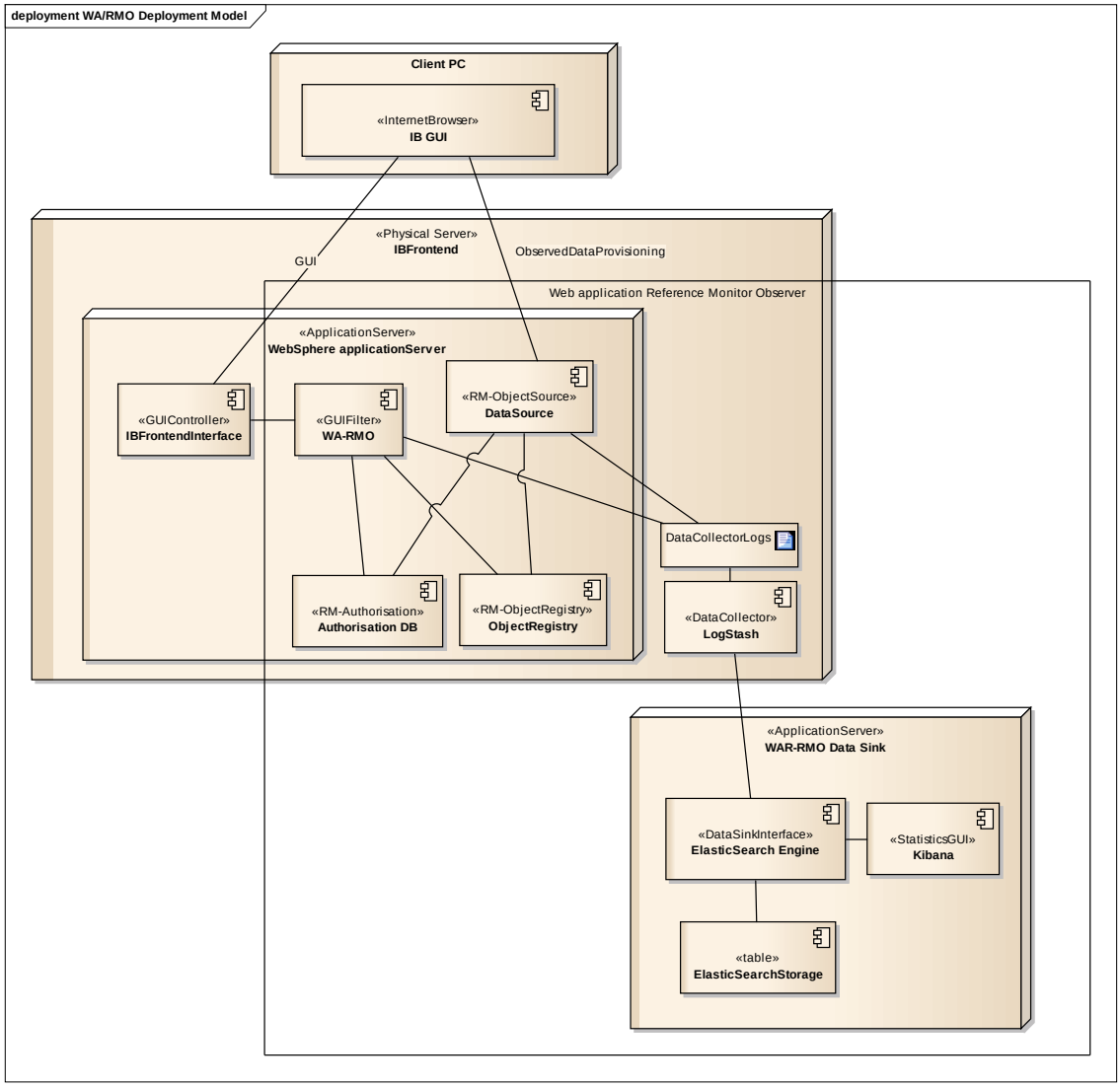
Hodnotitel	**P**	**R**	**A_1**	**G**	**M**	**A_2**	**T**	**I**	**C**	**All [%]**
H1	85	92	95	95	83	73	90	90	65	85,33
H2	88	95	95	95	70	95	86	95	75	88,22
H3	92	95	95	90	95	65	90	90	40	83,56
Prům (H)	88,33	94,00	95,00	93,33	82,67	77,67	88,67	91,67	60,00	**85,70**

Zdroj: vlastní zpracování na základě hodnot H1..H3

10. 7 Design měřicí sondy WA-RMO a jeho integrace

Design měřicí soundy a její integrace do předmětu měření (webové aplikace) je prezentován jako deployment view formálně modelované jazykem UML – Deployment model. Pro přehlednost jsou komponenty nástroje WA-RMO umístěny v oblasti „*WEB application Reference Monitor Observer*“.

Model nasazení WA-RMO do hodnocené aplikace



Zdroj: vlastní zpracování

10. 8 Konstrukt míry GQM, Organizace A, G2

A_APP1_INFOSEC_G2	
Specifikace cíle (G2)	Dlouhodobě snížit počet vlastníkem (E3) neoklasifikovaných (E2) informací (E1), které jsou zpracovávány, ukládány a přenášeny (E4) v rámci inhouse vyvíjených webových aplikací.
Zájmové skupiny	Odbor provozu a vývoje IT, Chief Information Security Officer, Obchodní vlastník aplikace
Definice cílové oblasti bezpečnostního modelu a souvisejících entit.	E1 – Informace E2 – Hodnota informace E3 – Vlastník informace E4 – Zpracovatel informace
Specifikace otázek	
Otázka (G2-Q1)	Kolik neoklasifikovaných informací je v konkrétní aplikaci ukládáno, zpracováváno a přenášeno.
Očekávaná odpověď (Q1)	V aplikaci InternetBanking je zpracováváno maximálně 20% neoklasifikovaných informací
Množina vazeb mezi entitami rozšířeného bezpečnostního modelu	E3 - E1 (Vlastník cení informace)
Množina tříd protiopatření standardu ISO 27002:2009	Sekce 8: Správa informačních aktiv, 8.1, 8.2. Třída ochranného opatření pro určení vlivu na C, I, A: KLASIF_RIZ_INF.
Specifikace měr	
Míra (G2-Q1-M1)	Relativní množství datových elementů webové aplikace, které na frontend úrovni jsou zpracovány a zobrazovány a nemají vlastníkem přiřazenu bezpečnostní klasifikaci ve všech případech užití.
Atribut (a1)	Počet zapsaných objektů (elementů datového modelu) v Reference Monitoru
Atribut (a2)	Počet čtených objektů (elementů datového modelu) z Reference Monitoru
Atribut (a3)	Počet otestovaných případů užití aplikace
Atribut (a4)	Počet případů užití aplikace
Základní míra (m1)	Počet datových elementů z datového modelu aplikace, které jsou přenášeny na klientskou stanici.
Metoda měření (m1)	Diferenciální analýza TCB vs. webová aplikace metodou Reference monitoru, viz Design nástroje WAR-RMO.
Základní míra (m2)	Počet datových elementů z datového modelu aplikace, které jsou na klientské stanici zobrazovány a zpracovávány neautorizovaným subjektem.
Metoda měření (m2)	Diferenciální analýza TCB vs. webová aplikace metodou Reference monitoru, viz Design nástroje WAR-RMO.
Odvozená míra a měřicí funkce	$\mu_{G2_{Q1}} = \frac{m2}{m1}$
Indikátor a analytický model	Web application information leakage, G2-Q1-M1 < 20%
Zhodnocení míry	
Metoda hodnocení míry, hodnotitelé a kritéria pro akceptaci míry.	PRAGMATIC, 3 hodnotitelé, jména na žádost neuvedena H1 - IT specialista H2 - Security Architect H3 - Obchodní vlastník aplikace Kritérium pro akceptaci míry: *Avg(All) > 80%*
Skóre míry	Viz Skórovací karta PRAGMATIC

Výsledek akceptace míry	AKCEPTOVÁNA podle kritéria pro akceptaci míry, **Skóre = 87,19%**

Zdroj: vlastní zpracování

Skórovací karta PRAGMATIC

	P	**R**	**A_1**	**G**	**M**	**A_2**	**T**	**I**	**C**	**All [%]**
H1	90	92	95	95	85	70	95	95	80	88,56
H2	95	94	95	93	70	95	80	90	75	87,44
H3	95	95	95	90	95	70	95	95	40	85,56
Prům(H)	93,33	93,67	95,00	92,67	83,33	78,33	90,00	93,33	65,00	**87,19**

Zdroj: vlastní zpracování na základě hodnocení H1..H3

10. 9 Konstrukt míry GQM, Organizace B, G1

C_EMAIL_INFOSEC_G1	
Specifikace cíle (G1)	Dlouhodobě zajistit, aby zpracovatel informace (E4) identicky cenil hodnotu (E2) informace (E1) přenášené kanálem email a aplikoval stejná opatření, jaká vynucuje vlastník (E3) při komunikaci emailem.
Zájmové skupiny	Chief Information Security Officer, Chief Executive Officer
Definice cílové oblasti bezpečnostního modelu a souvisejících entit.	E1 – Informace E2 – Hodnota informace E3 – Vlastník informace E4 – Zpracovatel informace
Specifikace otázek	
Otázka (G1-Q1)	Kolik odeslaných emailů není označeno požadovanou bezpečnostní klasifikací? Kolik emailů není ochráněno před tím, než jsou odeslány ?
Očekávaná odpověď (Q1)	Emailovým kanálem odchází maximálně 2% neoklasifikovaných emailových zpráv.
Množina vazeb mezi entitami rozšířeného bezpečnostního modelu	E3 - E1 (Vlastník cení informace) E4 - E1 (Zpracovatel cení informace)
Množina tříd protiopatření standardu ISO 27002:2009	Sekce 8: Správa informačních aktiv, 8.1, 8.2. Třída ochranného opatření pro určení vlivu na C, I, A: RIZ_PRISTUP
Specifikace měr	
Míra (G1-Q1-M1)	Relativní množství odeslaných emailových zpráv, které nemají odesilatelem přiřazenu bezpečnostní klasifikaci.
Atribut (a1)	Počet zapsaných objektů (emailových zpráv) v Reference Monitoru
Atribut (a2)	Počet záznamů v autorizační DB pro zapsaný objekt (emailovou zprávu)
Atribut (a4)	Sledovaní odesilatelé
Atribut (a5)	Odeslané emailové zprávy
Základní míra (m1)	Počet emailů odeslaných na vybranou podmnožinu adres bez přiřazené klasifikace a ochrany
Metoda měření (m1)	Diferenciální analýza TCB vs. auditní stopa emailového systému.
Základní míra (m2)	Kolik emailů bez přiřazené klasifikace je odesláno na subjekt, který nemá přiřazenu identitu v autorizační databázi?
Metoda měření (m2)	Diferenciální analýza TCB vs. uživatel.
Základní míra (m3)	Počet odesílajících zaměstnanců
Metoda měření (m3)	Auditní stopa emailového systému.
Odvozená míra a měřicí funkce	$\mu_{G1_{Q1}} = \frac{\frac{m2}{m1}}{m3}$
Indikátor a analytický model	Email application leakage, G1-Q1-M1 < 2%
Zhodnocení míry	
Metoda hodnocení míry, hodnotitelé a kritéria pro akceptaci míry.	PRAGMATIC, 2 hodnotitelé, jména na žádost neuvedena H1 - IT specialista H2 - CISO Kritérium pro akceptaci míry: *Avg(All) > 80%*
Skóre míry	Viz Skórovací karta PRAGMATIC
Výsledek akceptace míry	AKCEPTOVÁNA podle kritéria pro akceptaci míry, **Skóre = 89,78%**

Zdroj: vlastní zpracování

Skórovací karta PRAGMATIC

	P	**R**	**A_1**	**G**	**M**	**A_2**	**T**	**I**	**C**	**All**
H1	70	95	80	95	90	80	100	90	80	86,67
H2	95	99	95	95	95	95	95	90	77	92,89
Prům(H)	82,50	97,00	87,50	95,00	92,50	87,50	97,50	90,00	78,50	**89,78**

Zdroj: vlastní zpracování na základě hodnot H1..H2