VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH WEBOVÉ APLIKACE PRO ANALÝZU RIZIK
THE WEB APPLICATION DESIGN FOR RISK ANALYSIS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Lenka Krýzová**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Lenka Krýzová**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2019/20

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh webové aplikace pro analýzu rizik

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrh řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

V rámci této práce student zhodnotí stávající stav procesu analyzování rizik ve zvolené společnosti. Následně vytvoří návrh webové aplikace pro usnadnění tohoto pracovního procesu a integrace aplikace do informačního systému společnosti. Součástí práce je také vytvoření manuálu pro obsluhu navrhované aplikace a finanční ohodnocení vývoje a provozu.

Základní literární prameny:

ČSN ISO/IEC 27000 (36 9797) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

ČSN ISO/IEC 27001 (36 9790) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010.

ČSN ISO/IEC 27005 (36 9790) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Řízení rizik bezpečnosti informací. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

DOUCEK, Petr. Řízení bezpečnosti informací. 2. rozš. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Diplomová práce se zabývá návrhem webové aplikace pro analyzování rizik, což usnadní provoz systému řízení bezpečnosti informací pracovníkům společnosti. Teoretická část diplomové práce vymezuje cíle práce, metodiky zpracování a principy programování ve využitých programovacích jazycích. Analytická část práce popisuje současný stav a analyzuje prostředí společnosti. Návrhová část pak obsahuje vlastní návrh webové aplikace, manuál pro obsluhu, postupy integrace do informačního systému společnosti a finanční ohodnocení.

Klíčová slova

analýza rizik, ISMS, webová aplikace, HTML, PHP, MySQL databáze

Abstract

The master's thesis is focused on the design of a web application which aims at facilitating maintenance of the organization information security management system. The theoretical part of the thesis includes an explanation of the used methods and programming principles. The analytical part defines the current state and the environment of the organization. The design part describes the web application development and integration process, represents an operating manual and financially evaluates application development and maintenance.

Key words

risk analysis, ISMS, web application, HTML, PHP, MySQL database

Bibliografická citace

KRÝZOVÁ, Lenka. *Návrh webové aplikace pro analýzu rizik.* Brno, 2020. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/127735. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne ……

……

podpis autora

Poděkování

Ráda bych tímto poděkovala panu inženýru Petru Sedlákovi za konzultace a poznámky ke zpracování této diplomové práce, a také za velmi cenné rady do profesního života. Dále bych ráda poděkovala oponentovi této práce, inženýru Vlastimilu Svobodovi. V neposlední řadě děkuji rodině, že mi studium na vysoké škole umožnila.

OBSAH

ÚVOD

V úvodní části diplomové práce popíšeme problematiku této práce. Úkolem autorky je navrhnout webovou aplikaci na analýzu informačních rizik, které mohou vzniknout v oblasti bezpečnosti informací. Aplikace využívá pragmatickou analýzu rizik stanovenou dle případu z reálného prostředí oddělení Kolejnet kde se mnoho informačních rizik vyskytuje, pro vývoj a testování, její návrh by však měl být obecněji uplatnitelný i v jiných případech. Toto zobecnění platí také proto, že aplikace bude využívat standardizovaných postupů a prvků definovaných v normách.

Celé řešení by mělo být řízeno jako projekt, neboť je to specifická neopakovatelná činnost. V hodnoceném oddělení však chybí prvky projektového řízení, a proto při řešení nebudou použity striktně všechny jeho metody a postupy. Teoretickou část použijeme jako vstupy pro analytické i návrhové kapitoly. Vypracovaná analýza pak bude sloužit především pro návrhovou část práce.

K řešení využijeme různé softwarové nástroje, různé prostředky a programovací jazyky a jejich kombinace. Webová aplikace vyžaduje provoz vlastní infrastruktury, v případě že nechceme investovat do licencovaných produktů či dodavatelského řešení, s tím vyvstává i problém kompatibility různého softwaru, na který bude při návrhu řešení brán ohled. V závěru práce provedeme také finanční ohodnocení nákladů na všechny stanovené činnosti.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Následující kapitola popisuje, čeho chceme v této práci dosáhnout a jaké metody k řešení využijeme.

1.1. Cíl práce

Cílem práce je vytvořit webovou aplikaci na analyzování rizik jako funkční součást systému řízení bezpečnosti informací, podle řady norem ISO/IEC 27000. Tato aplikace bude vyvíjena jako částečně automatizovaná, zejména z důvodu opakujících se výpočtů a skladování dat. Zároveň je v aplikaci zachován zásah lidského faktoru. Práce obsahuje také zpracovanou metodiku používání aplikace a návrh na integraci do informačního systému.

1.2. Metody a postupy zpracování

Vzhledem k faktu, že se jedná o strategickou změnu, budujeme webovou aplikaci na základě výstupů z různých analytických technik. Při postupu zpracování závěrečné práce se stává klíčovou činností získání vstupních dat pro testovací databázi, z toho důvodu byla na reálných datech provedena pragmatická neboli orientační analýza rizik pomocí tabulkového procesoru, a tato data byla využívána po celou dobu vývoje, případně pro testování. Vstupní data obsahují také seznam základních bezpečnostních hrozeb získaných v normě, který lze záměrně rozšířit o individuální hrozby. Zajištění komunikace mezi prvky, a také zpracovávání uživatelských požadavků, vyžaduje provoz webového serveru, v tomto případě jsme pro vývoj zvolili softwarový webový server Apache. Po vytvoření databáze s příslušnými tabulkami je nutné připojit další prvky jako HTML dokumenty a PHP skripty, pro něž bylo vytvořeno jednotné uživatelské rozhraní, doplněné webovou grafikou pomocí Kaskádových stylů. Po dokončení práce na aplikaci bude vytvořen manuál pro obsluhu této aplikace. Vývoj a provoz bude finančně vyhodnocen v nákladové tabulce v návrhové kapitole. Do návrhové kapitoly bude zařazena také integrace aplikace do informačního systému a prostředí organizace. [1][6]

TEORETICKÁ VÝCHODISKA PRÁCE

Zde uvedené teoretické poznatky využijeme v následujících kapitolách jako vstupy a podklady pro analyzování současného stavu i pro návrh řešení.

2.2. Obsah informační bezpečnosti

Obsahem této kapitoly je úvod do řešené problematiky bezpečnosti informací, a vyhodnocování rizik, které na tyto atributy působí nebo mohou působit. Různé organizace vlastní a spravují různá data a z nich sestavené informace, které mohou být cenné pro správné fungování organizace či zlepšování a určování strategie společnosti. Vedení společnosti by si mělo uvědomovat, že využití obou prvků v sobě zahrnuje značný ekonomický potenciál, a ovlivňuje nejen jednotlivé organizace, ale i celosvětový vývoj. Využití informačních technologií ale přináší i další druh trestné činnosti (kyberkriminalitu), s níž je potřeba se vypořádat, a také ji předcházet, aby neohrozila fungování společnosti. Opatření, které organizace přijímá pro zajištění bezpečnosti, by měla být přiměřená a účinná. [3]

Základní prvek ochrany před vznikem bezpečnostního incidentu, tedy stavu, kdy bezpečnostní hrozba využije zranitelnosti aktiva a způsobí škodu, je prevence. Je důležité správně pochopit co virtuální prostředí neboli kyberprostor představuje, jak funguje, a jaké jeho součásti představují slabá místa. Nejzranitelnější článek je vnější síť Internet, jenž představuje celosvětovou počítačovou síť, která propojuje menší sítě pomocí sady protokolů, a umožňuje komunikaci mezi jednotlivými rovnocennými uzly bez hlavního řídícího centra. [3][11]

Kyberkriminalita a její řešení se často odlišují vysokou mírou tolerance či lhostejnosti ze strany společnosti a uživatelů, a velmi obtížnou identifikací pachatele. Právě koncoví uživatelé nejčastěji představují oběť útočníka, proto má smysl vzdělávat uživatele v oblasti bezpečnosti a udržovat jejich znalosti aktuální, vzhledem k vývoji informačních a komunikačních technologií. Na uživatele, kteří se věnují tomuto oboru v rámci své profese, jsou kladeny ještě vyšší nároky na školení. [3]

Obecným návodem, jak chránit informace a data v různých systémech poskytují normy ISO/IEC řady 27 000, představují nám systém řízení bezpečnosti informací (zkr. ISMS) a také nabízejí vhodné postupy, jak tento systém implementovat do organizace a jak ho

udržovat v provozu. Řízení bezpečnosti informací dle těchto norem či dokonce certifikace tohoto systému řízení může pozitivně ovlivňovat i dodavatelsko-odběratelské vztahy. [4]

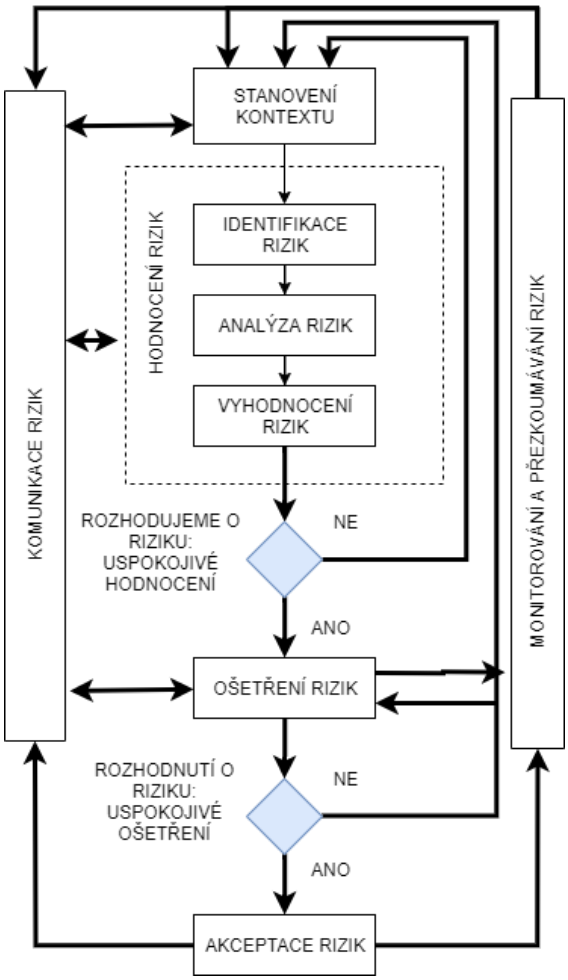
2.3. Změny ve firmě

Pro správné nasazení systému řízení informační bezpečnosti je podstatné získat výborné povědomí o fungování organizace a všech součástí. Jedině tak lze stanovit hranice a kontext pro vytvoření účinného ISMS, v souvislosti s přiměřeným využitím finančních i lidských zdrojů, a to vše v reálném čase. Moderní doba vyžaduje rychlý rozvoj a adaptaci vůči změnám, tímto způsobem můžeme eliminovat příčiny neúspěchu v podnikání. S rozvojem podnikání ale přichází také nutnost přizpůsobovat stupeň specializace zaměstnanců a jasně definovat řídící mechanismus, včetně optimálně vytvořené firemní byrokracie. Úspěch podmiňují faktory zahrnuté do rámce 7S faktorů firmy MC Kinsey. V případě, že se v podniku vyskytne změna, ať už plánovaná nebo neočekávaná, je přinejmenším vhodné, aby se jednalo o změnu řízenou. V obou případech tedy při řízení změn sledujeme externí i interní faktory, používáme různé strategie a postupy, a reagujeme způsobem, který odpovídá vizi společnosti. Obecným cílem je vždy udržet společnost efektivní, životaschopnou a konkurenceschopnou. Takzvaný Lewinův model definuje jednotlivé fáze procesu řízené změny v podniku. Proces změny v tomto modelu chápeme jako projekt, který je specifikovaný omezenými zdroji, časem i konkrétními procesy a výsledky, které jsou měřitelné. Součástí takového projektu jsou i vhodně zvolené analýzy. [14]

2.4. Řízení rizik

Abychom vytvořili efektivní systém řízení bezpečnosti informací (ISMS) je nutné zavést do organizace systematický přístup také k řízení rizik. Řízení rizik informační bezpečnosti by mělo být v souladu s celkovým řízením rizik organizace (celková rizika lze řídit podle norem řady ISO/IEC 31 000), a mělo by být přizpůsobeno prostředí organizace, její části nebo například informačnímu systému. Jedná se o nepřetržitý proces, kdy stanovujeme kontext, vyhodnocujeme a ošetřujeme rizika. Norma ISO/IEC 27 005 se zaměřuje na problematiku řízení informačních rizik, a je tak podpůrným dokumentem, jak pro zavádění a udržování komplexního ISMS, tak také pro návrh

částečně automatizovaného nástroje analýzy rizik, kterému se budeme věnovat v této práci. [6]



Obrázek 1: proces řízení rizik bezpečnosti informací (Vlastní zpracování dle [6])

Z obrázku výše vyplývá, že řízení rizik a všechny jeho prvky jsou cyklickými procesy. Normy kladou důraz nejen na správné zavedení ISMS ale také na jeho udržování, kontrolu a aktualizaci podle Demingova PDCA diagramu, totéž platí pro činnosti řízení rizik bezpečnosti informací. [6]

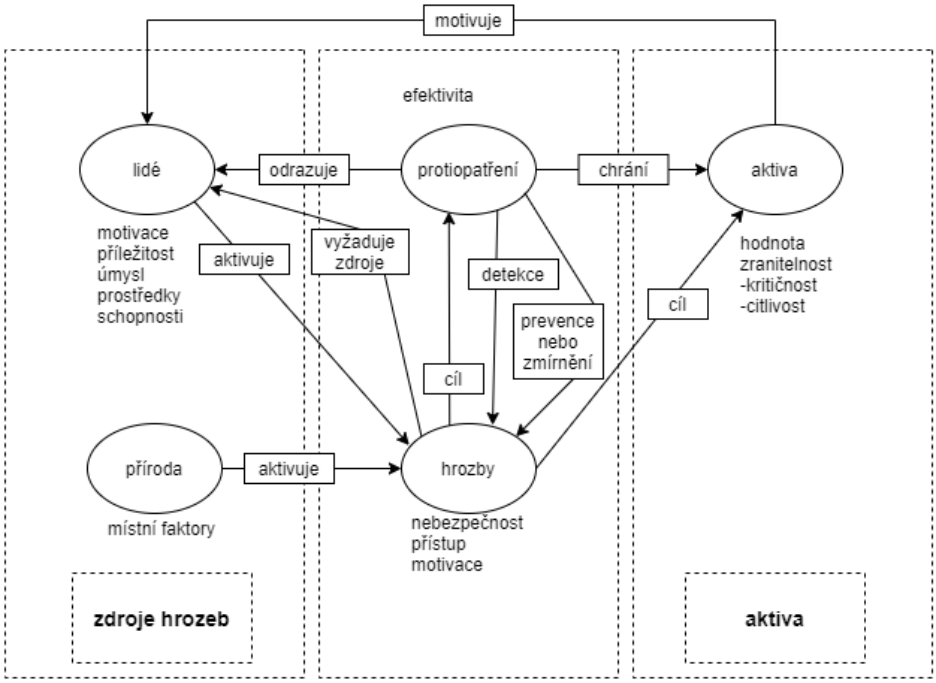
Tabulka 1: propojení ISMS a řízení rizik (Vlastní zpracování dle: [6])

ISMS proces	PDCA proces	proces řízení rizik bezpečnosti informací
PLÁNUJ	PLAN	stanovení kontextu, posouzení rizik, příprava plánu ošetření rizik, akceptace rizik
DĚLEJ	DO	implementace plánu ošetření rizik
KONTROLUJ	CHECK	kontinuální monitorování a přezkoumávání rizik
JEDNEJ	ACT	udržování a zlepšování procesu řízení rizik

Nelze jednoznačně definovat pojem riziko, obecně se však podle Raise jedná o *„vystavení nepříznivým okolnostem“*, či *„odchýlení skutečných a očekávaných výsledků“* apod. Existuje mnoho druhů rizik, zaměřujících se na různé oblasti. Každé riziko definuje jeho neurčitý výsledek, přičemž existují dvě varianty tohoto výsledku, z nichž alespoň jedna je nežádoucí. [14]

Analyzujeme-li rizika, procházíme prvním krokem procesu snižování rizik. V tomto kroku obvykle stanovujeme hrozby, pravděpodobnost uskutečnění hrozeb a dopad těchto hrozeb na aktiva, tímto definujeme rizika a jejich závažnost. Při analýze obecně nejprve identifikujeme aktiva, které vymezený subjekt vlastní, následně stanovíme hodnoty aktiv a jejich význam pro subjekt, dále identifikujeme hrozby a slabiny, které mohou negativně ovlivnit aktiva, a nakonec stanovíme závažnost hrozeb a míry zranitelnosti subjektu vůči dané hrozbě. Získané výsledky napomáhají k určení a realizaci správných opatření proti výskytu či k omezení hrozeb. Zde platí, že kombinace více opatření je vždy účinnější, než pouze jedno nasazené opatření. Obvykle nelze odstranit všechna rizika, ale vždy lze určit úroveň, na kterou analyzovaná rizika eliminujeme. Pro zbytková rizika není nutné určovat opatření k jejich snížení. [14]

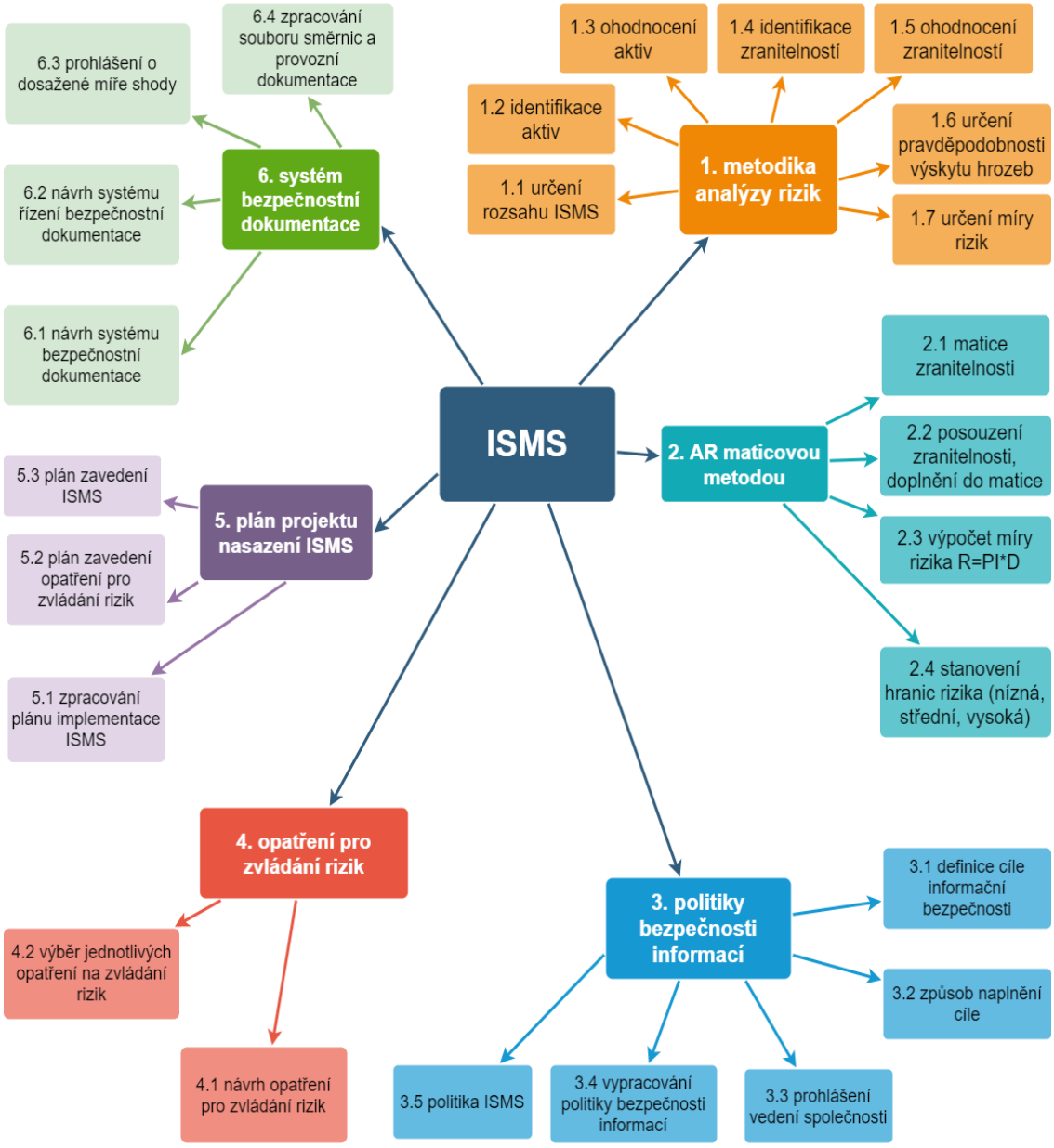
Abychom úspěšně provedli analýzu rizik, je vhodné důkladně prozkoumat a pochopit vztahy a souvislosti mezi jednotlivými prvky, tyto vztahy zobrazuje obrázek č. 2.



Obrázek 2: vztahy v analýze rizik (Zdroj: [14])

2.5. Stanovení kontextu

Tato část potřebuje jako vstupy veškeré informace o organizaci, na těchto základech pak můžou být určena kritéria pro řízení rizik informační bezpečnosti, je definován rozsah a hranice a je také stanovena příslušná organizační struktura pro řízení rizik bezpečnosti informací. Primární je určení účelu řízení rizik, kdy v případě této práce uvažujeme systém řízení rizik za podpůrnou součást ISMS a webovou aplikaci pak jako nástroj systému řízení rizik informační bezpečnosti. [6]



Obrázek 3: vizualizace částí ISMS dle ISO/IEC norem řady 27 000 (Zdroj: [6])

2.5.1. Rozsah a hranice

Stanovení rozsahu procesu řízení rizik musí být provedeno, aby bylo zajištěno, že jsou brána v úvahu všechna příslušná aktiva. Také identifikujeme hranice k řešení rizik, která by mohla tyto hranice prolomit. Oddělíme tak aktiva, která budou zahrnuta do analýzy rizik od těch, které nezahrneme. Při stanovování uvažujeme ovlivňující faktory jako jsou:

- strategické obchodní cíle, strategie a politiky organizace,
- obchodní procesy,
- funkce a struktura organizace,
- právní, regulační a smluvní požadavky platné pro organizaci
- politika organizace týkající se bezpečnosti informací,
- celkový přístup organizace k řízení rizik,
- informační aktiva,
- geografické charakteristiky sídla organizace,
- omezení ovlivňující organizaci,
- sociálně kulturní prostředí a jiné. [6][14]

2.5.2. Kritéria

V závislosti na zvoleném přístupu k řízení rizik a strategii organizace postupně vhodně stanovíme kritéria hodnocení a kategorizace aktiv, hodnocení hrozeb a hodnocení rizik, kritéria dopadu a kritéria akceptace rizik. [6]

2.6. Posouzení rizik

Norma definuje posuzování rizik jako proces v organizaci, který se sestává z činností jako identifikace rizik, analýza rizik a hodnocení rizik. Rizika by zde měla být identifikována, popsána (kvalitativně nebo kvantitativně) a prioritizována na základě stanovených kritérií a cílů. Podrobnější popis postupu analýzy informačních rizik nabídnou následující kapitoly, vždy však musíme uvažovat nad analýzou ve stanoveném kontextu. [6]

2.6.1. Identifikace

„Účelem identifikace rizik je určit, co by se mohlo stát, aby byla způsobena potenciální ztráta, a porozumět tomu jak, kde a proč ke ztrátě může dojít.“ [6]

Tento proces dále dělíme na činnost identifikace aktiv (kdy je výstupem seznam aktiv organizace, u nichž je třeba zajistit řízení rizik), identifikace hrozeb, identifikace stávajících opatření, identifikace zranitelností, jež mohou být zneužity hrozbami a identifikace následků (jako seznam scénářů incidentů s jejich následky). [6]

2.6.2. Analýza

Kvalitativní nebo kvantitativní analýza rizik je pak prováděna na základě určité metodiky a v různých stupních podrobnosti, v závislosti na rozsahu známé zranitelnosti, kritičnosti aktiv a předcházejících incidentech. Následuje proces posouzení následků, a to vzhledem k hodnotě za náhradu aktiva nebo hodnotě obchodních následků ztráty nebo kompromitace aktiva. Výstupem další činnosti jsou určené pravděpodobnosti scénářů incidentů, a dále také určení úrovně rizik. V obou případech hodnotíme opět kvalitativně nebo kvantitativně. Odhadnuté riziko je rovno kombinaci pravděpodobnosti scénáře incidentu a jeho následků neboli dopadu. [6]

2.6.3. Hodnocení

V posledním kroku tohoto procesu provádíme hodnocení rizik (prioritizaci). Dle hodnocení rozhodujeme o dalších krocích (např. zda by měla být činnost prováděna či omezena) a bereme přitom v úvahu také smluvní, právní a regulační požadavky. Na základě priorit také určujeme použitá opatření. [6]

2.7. Ošetření a akceptace rizik

Při ošetřování rizik použijeme výstupy z části posuzování rizik, hodnoty předpokládaných nákladů na ošetření rizika a také hodnoty očekávaných přínosů, vyplývajících ze způsobů ošetření rizika. Snížení nepříznivých výsledků rizik na nejnižší dosažitelnou míru by ale mělo být přiměřené a měly by být také zohledněny názory zúčastněných stran. Činnosti spojené s ošetřením rizik jsou modifikace, podstoupení, sdílení a vyhnutí se riziku. Výstupem této části je dokumentovaný plán ošetření rizik. [6]

2.8. Komunikace a konzultace rizik bezpečnosti informací

Základem této kapitoly je komunikace výsledků posuzování rizik se zainteresovanými stranami, tyto strany mohou mít vliv na rozhodování, které z výsledků vyplývá. [6]

2.9. Monitorování a přezkoumání rizik bezpečnosti informací

Vzhledem k faktu, že rizika nejsou stálá, mohou se všechny části analýzy i její výsledky měnit. Průběžné sledování stavu bezpečnosti (vnitřní i vnější) a detekce změn je proto nezbytná. Stejně tak zajištění dostupnosti všech zdrojů informací pro posouzení a ošetření, přezkoumávání všech částí řízení rizik a platnosti kritérií jsou zásadní činnosti, které mohou vést k aktualizaci či změně použitého přístupu. Příslušným způsobem by mělo být o všech krocích informováno vedení, stejně tak jako o jakémkoli jiném podstatném kroku, během celého procesu. Obecně tato kapitola tedy cílí na neustálou platnost procesu řízení informačních rizik se vztahem k obchodním cílům organizace. [6]

2.10. Vývoj webové aplikace

Vývoj webové aplikace vyžaduje znalost několika základních prvků tvorby webu. Úspěšný projekt znamená několik následujících dobře promyšlených bodů:

- promyšlený, realistický a vhodně zvolený projekt,
- využitelnost či přínos projektu,
- technologické zázemí,
- vývojářský tým,
- dostačující funkčnost webové aplikace,
- dobrou dostupnost,
- moderní grafický design. [11]

Se všemi těmito body souvisí využití vhodných technologií. V našem případě je výběr omezen technologiemi používanými v oddělení, vhodně tak využijeme programovací jazyk HTML, PHP a JavaScript, pro databázové prvky využijeme MariaDB, nástupce MySQL s otevřeným kódem. Kaskádové styly neboli CSS využijeme pro definování grafických prvků webové aplikace. [11][17]

Po zamyšlení, jak bude projekt zhruba vypadat a jakým způsobem jej budeme řídit, navrhneme strukturu webu a tím určíme rozdělení souborů do složek. Struktura by neměla obsahovat všechny soubory v jedné složce, ale spíše několik podsložek v kořenové složce webových stránek, které se tak stávají přehlednější. Odděleně budeme uchovávat například dokumenty Kaskádových stylů a všechny obrázkové dokumenty. Jména složek i souborů by měla být věcná, krátká a psaná bez diakritiky a speciálních znaků. Servery

s operačními systémy s jádrem Unix či Linux rozlišují v názvech souborů velká a malá písmena, proto bychom se měli psaní velkých písmen vyvarovat, abychom udrželi přehlednost webu. [11]

Je vhodné také používat relativní odkazování pro soubory v rámci webové prezentace na jednom serveru. Jako výchozí adresář je vždy míněn soubor, ze kterého odkazujeme a v případě odkazování na jiný server používáme úplnou specifikaci cesty. Umožníme tak snadný přenos celého webu na jiný server. Výchozí soubor webové prezentace je nejčastěji označován jako index.html nebo index.php. [11]

Pro snadnější psaní a správu všech částí webové prezentace využijeme hned několik různých softwarových nástrojů. Použitím strukturálního editoru pro vytváření HTML a PHP stránek si usnadníme psaní kódu, protože tyto editory poskytují na rozdíl od běžných textových editorů zvýraznění a kontrolu syntaxe, kontrolu validity, automatické doplňování či mnoho vývojářských funkcí a nástrojů. Příkladem takového multi-jazykového editoru je PSPad, který byl vyvinut v České republice a je distribuován bezplatně. Pro grafické aplikace se hojně využívá software Adobe Photoshop případně Adobe Illustrator, ten je částečně pro webovou grafiku přizpůsoben (umožňuje řezy, paletu barev RGB i rozvržení velikosti plátna v pixelech). [11]

Velmi užitečný je program Total Commander, tento pomocník je nejen výborný správce souborů, ale také přehledný FTP klient. File Transfer Protocol (FTP) je nejrozšířenější protokol pro kopírování souborů, tvořící obsah webu, na webový server pomocí tzv. FTP klienta. Pro testování zobrazení a funkčnosti webových stránek využijeme internetové prohlížeče. Je vhodné jich použít několik a přesvědčit se tak, o správnosti zobrazování. Mezi nejznámější internetové prohlížeče řadíme Internet Explorer, Mozilla Firefox, Google Chrome a Opera, většina těchto prohlížečů má již integrované vývojářské nástroje. Důležitým krokem je validace syntaxe, tímto postupem opravujeme chyby v kódu u všech dokumentů. Využít můžeme výše zmíněné vývojářské nástroje či web oficiálního validátoru konsorcia W3C. [11]

Jazyk HTML a jeho zdrojové kódy sice mají přesnou syntaxi, jsou ale velmi přizpůsobivé, a i přes chyby v kódu internetové prohlížeče obvykle dokážou zobrazovat webové stránky správně. Zdrojový kód je vždy pouze v textovém formátu ASCII, v tomto formátu je interpretován prohlížečem a není kompilován do žádného z binárních souborů, jako je tomu u běžných programovacích jazyků. Na binární soubory, obrázky a multimédia

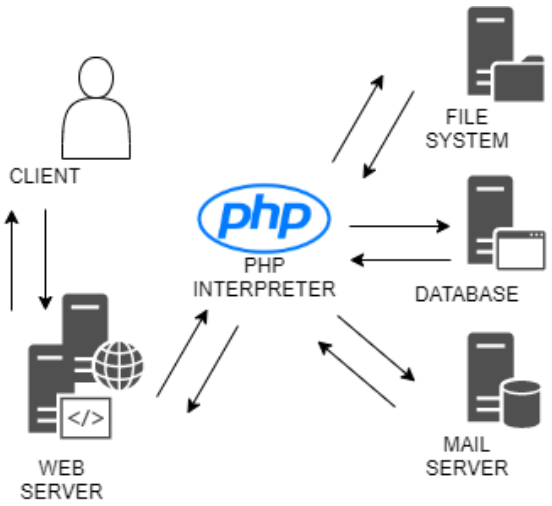
v externích souborech se pouze odkazujeme. Příkazy jazyka HTML uzavíráme do párových či nepárových značek v určité struktuře dokumentu. [11]

```
0         10        20        30        40        50        60        70
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
2 <html>
3   <head>
4   <meta http-equiv="content-type" content="text/html; charset=utf-8">
5   <meta name="generator" content="PSPad editor, www.pspad.com">
6   <title></title>
7   </head>
8   <body>
9
10  </body>
11 </html>
12
```

Obrázek 4: obecná struktura HTML dokumentu v PSPad (Zdroj: [11])

Kde DOCTYPE představuje informace, o jaký typ dokumentu se jedná, jakou verzi jazyka HTML dokument používá a jaké znaky (jazyk). HTML párová značka označuje začátek dokumentu HTML a HEAD představuje hlavičku dokumentu, která není zobrazována, ale obsahuje důležité informace o obsahu, autora, odkazy na Kaskádové styly atd., včetně titulku v horní liště prohlížeče TITLE a metatagů, kde upřesňujeme kódování, klíčová slova a jiné informace o dokumentu. Samotný obsah stránky pak zobrazuje párová značka BODY. [11]

V projektu využijeme také skriptovací jazyk PHP, je jednoduchý a podporuje funkce, podmínky a cykly. Na rozdíl od JavaScriptu, kdy ke zpracování dojde v prohlížeči, PHP skripty se zpracovávají na serveru. PHP se vyvinul jako strukturální programovací jazyk a postupně přešel také k objektovému modelu programování, tento model se však u vývojářů příliš neujal. [11]



Obrázek 5: základní funkční struktura PHP (Zdroj: [11])

Hlavními výhodami PHP jsou podpora řady technologií a standardů, výborná komunikace s webovým serverem Apache a databázemi jako MySQL, Oracle, MS SQL a jiné, je také multiplatformní a podporuje ho většina poskytovatelů webhostingu. I přesto je však například technologie Microsoft ASP.NET pro vývoj dynamických stránek pohodlnější, efektivnější a modernější, nicméně je pro provoz dražší. [11]

Relační databáze MariaDB je nástupnickou větví open source databázového systému MySQL. K přístupu k datům lze využít software phpMyAdmin, jehož grafické uživatelské rozhraní ulehčuje správu dat a je velmi přehledné. Využití kombinace technologií PHP a MySQL resp. MariaDB má hned několik výhod, jednoduchost a přenositelnost, obsáhlou dokumentaci, širokou podporu a komunitu, která udržuje mnoho diskuzních webů, kde lze snadno najít řešení nejednoho problému. Při psaní kódu bychom si měli osvojit uvádění komentářů, ty se zobrazují pouze ve zdrojovém kódu a umožňují práci s kódem také ostatním programátorům, ti získají přehled o tom, co které části a funkce představují. [11][17]

Během programování využijeme několik následujících pravidel:

- V HTML dokumentu píšeme PHP kód mezi znaky `<?PHP` a `?>`.
- Proměnné se v jazyce PHP označují symbolem `$` a názvem, příklad `$vysledek`, deklarace probíhá v průběhu kódu a hodnoty přiřazujeme rovnítkem.
- Prvek `echo` dokáže vypisovat proměnné či textové řetězce na obrazovku (podobně jako příkaz `print`).
- Píšeme-li samostatně textové řetězce ohraničujeme je do dvojitých uvozovek.
- Podmínky využíváme současně s příkazem `if`, jeho struktura je následující:

```
3  if (podmínka 1)
4  {
5      příkaz 1;
6      příkaz 1.2;...
7  }
8  elseif (podmínka 2)
9  {
10     příkaz 2;
11     příkaz 2.2;...
12 }
13 else
14 {
15     příkaz 3;
16     příkaz 3.1;...
17
18 }
```

Obrázek 6: struktura příkazu IF (Zdroj: [11])

- Jako metody odesílání dat mezi skripty upřednostníme POST oproti GET. POST metoda je vhodnější pro odesílání citlivých dat z formulářů, neboť se odesílaná data neobjevují v URL adrese.
- Jednotlivé instrukce oddělujeme vždy středníkem.
- Uvažujeme nad tím, jaké mají proměnné datové typy a v případě potřeby provedeme přetypování.
- Logické operátory jsou následující:

Tabulka 2: logické operátory v PHP (Zdroj [11])

operátor	jiný zápis	význam	je pravda když
AND	&&	logický součin	jsou obě hodnoty pravdivé
OR	||	logický součet	alespoň jedna hodnota pravdivá
XOR		exkluzivní OR	právě jedna hodnota pravdivá
!		negace	PRAVDA pokud bylo NEPRAVDA a naopak

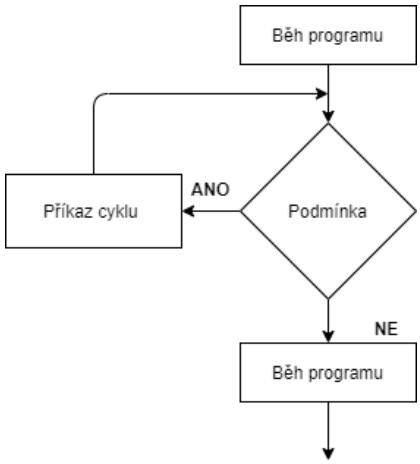
- Operátory porovnání jsou následující:

Tabulka 3: operátory porovnání v PHP (Zdroj: [11])

operátor	význam
>	větší
<	menší
=	rovno
>=	větší nebo rovno
<=	menší nebo rovno
<>	nerovnost
!=	nerovnost (jiný zápis)

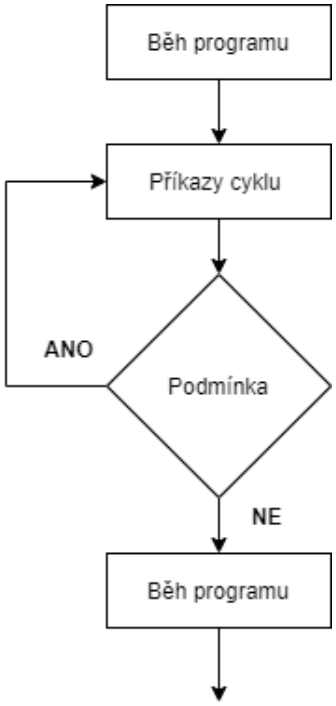
- Prioritu operátorů ve vzorcích definují kulaté závorky.
- Datový typ pole má prvky, a každý prvek v poli má index nebo klíč a hodnotu. Pole je tedy určeno indexem (číselně), v případě asociativního pole jsou ale prvky rozlišeny textovým řetězcem.
- U vícerozměrných polí označuje první hodnota v hranaté závorce index řádku a druhá hodnota v hranaté závorce index sloupce.

- Pro inicializaci pole používáme funkci `array()` nebo přiřazení jednotlivým indexům (př. `$pole[indexX][indexY] = “textový řetězec či hodnota“;`)
- Pro opakované vyhodnocování stejného výrazu, s rozhodováním na základě jeho výsledné hodnoty, použijeme příkaz `SWITCH` nebo `IF`.
- Cyklus s podmínkou na začátku otestuje výraz a dokud je platný, provádí se série příkazů. Pro tyto případy použijeme cyklus `WHILE.`



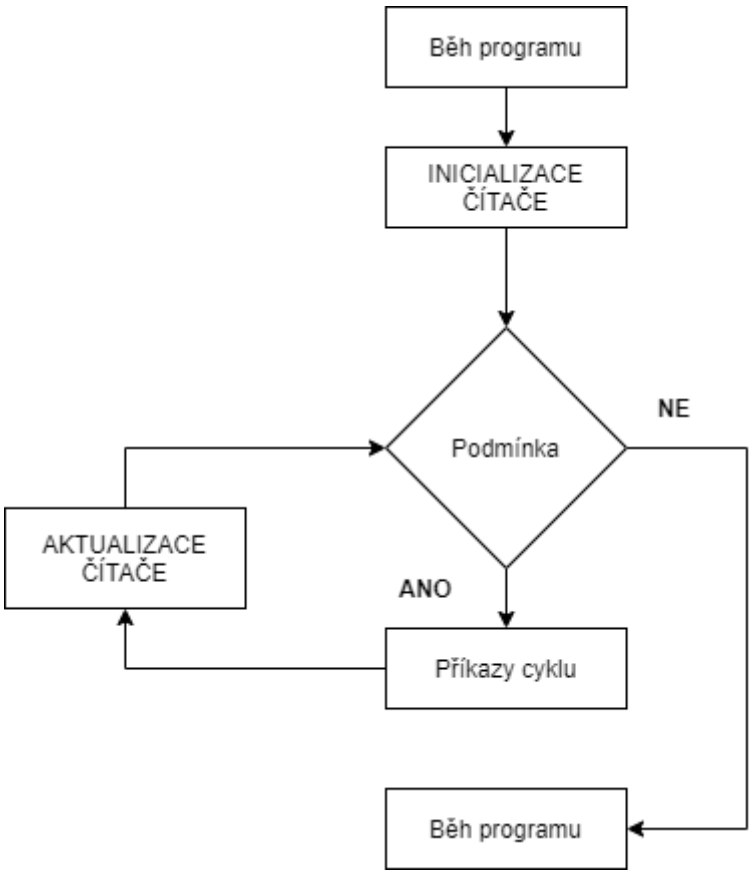
Obrázek 7: schéma cyklu s podmínkou na začátku (Zdroj [11])

- Cyklus s podmínkou na konci jedenkrát provede příkaz a poté ověřuje podmínku.



Obrázek 8: schéma cyklu s podmínkou na začátku (Zdroj: [11])

- Cyklus s řídící proměnnou, kde je předem definovaný počet opakování cyklu, provedeme pomocí `FOR`.



Obrázek 9: schéma cyklu s definovaným počtem opakování FOR (Zdroj: [11])

- Využíváme funkce, které oproti procedurám vrací hodnotu. Deklarujeme je s klíčovým slovem `function`, rozlišujeme je názvem a tělo oddělujeme složenými závorkami. Klíčové slovo `return` označuje, co má funkce vracet.
- Využíváme také vnitřní funkce, jazyk PHP jich nabízí dostatek.
- V tzv. PHP manuálu nalezneme dostatek informací, i rad od zkušených uživatelů.
- Pro připojení k databázi musí být definováno několik údajů, zejména název hostitele, číslo portu, na kterém databáze naslouchá, název databáze, uživatelské jméno a heslo.
- Pro práci s daty využíváme příkazy dotazovacího jazyka SQL a jeho podmnožinu pro manipulaci s daty DML.
- Mezi příkazy jazyka DML řadíme zejména `SELECT` pro výběr dat, `INSERT` pro vkládání dat, `DELETE` pro mazání dat či `UPDATE` pro aktualizaci dat.

```sql
SELECT
    seznam požadovaných položek
FROM
    seznam tabulek
WHERE
    podmínka
GROUP BY
    seznam položek
HAVING
    skupinová podmínka
ORDER BY
    třídění;
```

Obrázek 10: základní struktura SQL příkazu SELECT (Zdroj: [11])

- Dále využíváme jazyka DDL pro definování a úpravy databázových struktur. Používáme příkazy jako `CREATE DATABASE`, `CREATE TABLE`, `ALTER TABLE`, `DROP TABLE` a jiné.
- Databáze obecně představuje danou uspořádanou množinu dat či informací, umístěnou na paměťovém médiu. Uložená data jsou konzistentní, je zajištěna integrita databáze pomocí integritních omezení.
- V databázi popisujeme množiny prvků tzv. objekty. Entitami rozumíme libovolné existující objekty reálného světa a jako atributy entity označujeme jejich charakteristiky či vlastnosti.
- Databázové tabulky spojují relace na základě stanoveného klíče (primární klíč, cizí klíč, složený primární klíč), který jednoznačně identifikuje záznam.
- Popis datových struktur a vazeb v databázi uvádí datový model, pro návrh struktury databáze lze využít E-R diagram. [11]

Tento výpis samozřejmě není kompletní návod, jak programovat ve zmíněných jazycích, zahrnuje ale významné prvky potřebné ke správnému návrhu této webové aplikace. Kompletní dokumentaci pro jazyk PHP lze dohledat na následující webové adrese https://www.php.net/docs.php. Další užitečný web pro vývojáře najdeme na adrese https://www.w3schools.com/. [11]

ANALÝZA SOUČASNÉHO STAVU

V této kapitole si nejprve představíme organizaci i hodnocené oddělení, a popíšeme informační systém, který je využíván. Následně provedeme sadu analýz, které jsou v tomto případě nezbytné, protože v oddělení provádíme strategickou interní změnu.

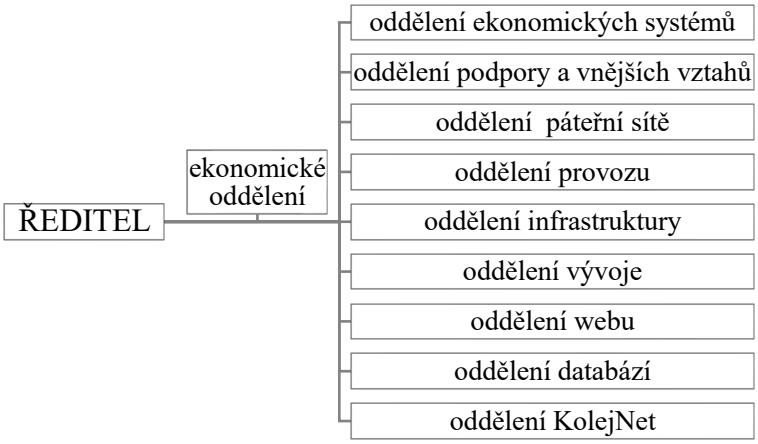
3.1. Studie organizace

Tato část definuje charakteristické prvky organizace. Vysoké učení technické v Brně je veřejná vysoká škola (univerzita) s osmi fakultami, několika vysokoškolskými ústavy a dalšími součástmi. Vysoká škola poskytuje výuku technických, ekonomických či uměleckých věd. Celkový počet studentů se v současnosti pohybuje okolo 20 tisíc, v bakalářských, magisterských a doktorských oborech. Hlavním účelem existence organizace je tedy vzdělávání, věda a výzkum, konkurence tohoto segmentu je obvykle lokalizována ve velkých městech, v rámci celého světa. Kulturu organizace a její obchodní činnosti definují jak osvědčené pracovní postupy zaměstnanců, tak také fakt, že se jedná o právnickou osobu zřizovanou zákonem a financovanou především dotacemi ze státního rozpočtu. Posláním takové organizace pak můžeme stanovit *„poskytování kvalitních veřejných služeb v oblasti vzdělávání“,* pod kontrolou Systému managementu kvality dle ČSN EN ISO 9001:2016 a etického kodexu. [9]

3.1.1. Popis vybraného oddělení

Vybrané oddělení KolejNet je součástí Centra výpočetních a informačních služeb (zkr. CVIS) při Vysokém učení technickém v Brně (dále jen VUT). Zázemí pro studenty poskytované Kolejemi a Menzami (KaM) při VUT v Brně rozšiřuje hodnocené oddělení KolejNet o služby připojení k internetu, které jsou nezbytné pro studium na vysoké škole. KolejNet představuje studentskou kolejní síť, jejíž předchůdce Listnet, vznikl v roce 1994 na Listových kolejích na Kounicově ulici v Brně. V roce 1999 byl Listnet transformován na síť KolejNet a stal se součástí technického oddělení KaM. Organizačně spadá oddělení KolejNet od roku 2005 pod CVIS VUT v Brně, které mimo jiné zajišťuje provoz a správu páteřní počítačové sítě, webových aplikací VUT, centrální databáze VUT a cloudových služeb pro VUT. Vztahy a řízení organizace upravuje Organizační řád VUT v aktuálním

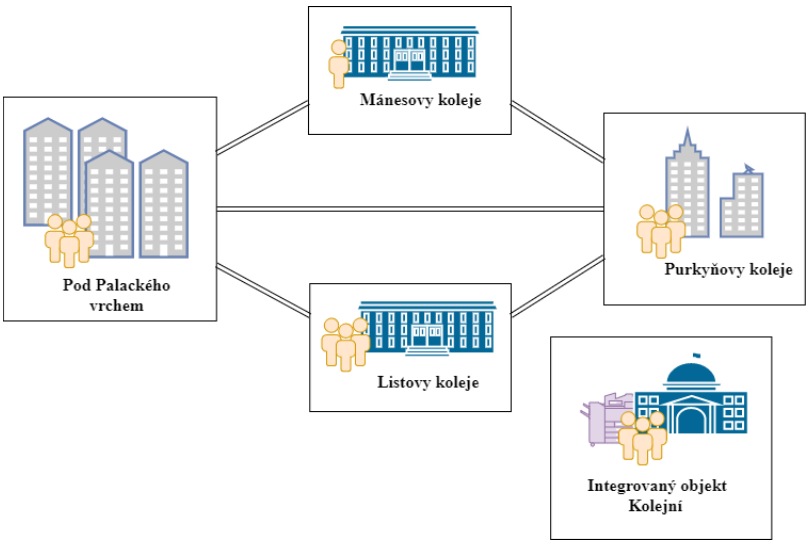
znění. Oddělení KolejNet zpracovává, podle dostupných údajů, asi 10 000 unikátních IP adres v rozdílném poměru IPv6 a IPv4. [8]



Obrázek 11: liniová organizační struktura CVIS (Zdroj: [8])

3.1.2. Prostředí oddělení

Oddělení KolejNet spravuje počítačovou síť, která pokrývá čtyři hlavní areály studentských kolejí VUT v Brně. Jednotlivé areály spojuje optická páteřní síť. Pro horizontální a pracovní sekce je použita metalická kabeláž. Tyto sekce spravuje celkem dvanáct zaměstnanců oddělení KolejNet. Je zde využívána technologie Gigabit Ethernet a koncové uzly jsou nejčastěji uživatelská zařízení různých druhů, vybavená různými operačními systémy. Provoz na síti nepřetržitě monitorují dohledové systémy, i tak se ale mohou vyskytovat bezpečnostní hrozby různého původu. Oddělení nemá zavedené žádné formální procesy či systém pro hodnocení a eliminaci informačních rizik.



Obrázek 12: rozložení areálů a jejich propojení (Vlastní zpracování)

Rozhodovací úroveň organizační struktury (zde liniové) stanovuje strategickou orientaci, která směřuje k efektivnímu dosahování poslání organizace, proto všechny podřízené plány (včetně zavádění ISMS a jeho částí) musí být těmto rozhodnutím podřízena. Koordinaci a řízení těchto procesů provádí vedoucí úroveň organizační struktury (vedoucí oddělení) a výrobní a podpůrné činnosti pak naplňuje operační úroveň (pověření zaměstnanci). Seznam vnitřních a vnějších omezení, které mohou ovlivnit celý systém ISMS a jeho provoz je následující:

- omezení zdrojů (lidské a finanční zdroje),
- omezení politického charakteru (financování ze státního rozpočtu v závislosti na rozhodnutí vlády a poslanecké sněmovny České republiky),
- funkční omezení (nerovnoměrná zátěž počítačové sítě během kalendářního roku, nejvyšší pak během akademického roku),
- personální omezení (odbornost a úroveň kvalifikace),
- technologická a technická omezení (možnosti kvality SW a HW vybavení vzhledem k ceně),
- prostorová omezení (zejména pro fyzickou bezpečnost),
- omezení kulturního charakteru a jiné (zahraniční uživatelé). [6]

3.1.3. Informační systém oddělení

Oddělení provozuje informační systém, který slouží jako centrální zdroj informací pro zákazníky i zaměstnance. Zákazníci jej využívají pro registraci připojení, evidenci a manipulaci s nabízenými službami a s kontaktními údaji. Jednofaktorová autentizace do informačního systému zahrnuje přihlašovací jméno a též vstupní heslo, které lze získat z informačního systému Kolejí a Menz VUT v Brně. Další data, včetně osobních údajů jsou importována z databázových systémů Kolejí a Menz VUT v Brně. Zaměstnanci využívají IS pro evidenci a správu uživatelských dat (včetně organizace přípojek), jako nástroj evidence a kontroly provozu síťových prvků (management prvků skrze webové rozhraní, pokud to prvky dovolují) a jako nástroj pro sledování stavu sítě (včetně logovacích funkcí). Podstatnou součástí jsou také služby elektronické pošty, skrze kterou jsou fakturovány služby zákazníkům a probíhá zde velká část komunikace mezi všemi zúčastněnými stranami. Informační systém je sestaven na míru potřebám oddělení, není

tedy využito licencovaného produktu. Informační systém je provozován na vlastní infrastruktuře umístěné v areálu Kolejí a Menz VUT v Brně.

3.2. Současné normativní ohraničení oddělení

Právním řádem je tomto případě myšlena veškerá právní úprava České republiky (tzn. Občanský zákoník, Zákoník práce atd.) a Evropské unie (GDPR a jiné.), kterou je organizace povinna dodržovat při své činnosti.

3.2.1. Vnitřní směrnice a pravidla

Včetně právního řádu se organizace řídí i dokumentovanými vnitřními pravidly. Následující tabulka shrnuje různé druhy vnitřních předpisů, směrnic a norem, které platí pro hodnocené oddělení.

Tabulka 4: současné vnitřní předpisy (Vlastní zpracování)

Traumatologický plán
Požární poplachové směrnice
Provozní bezpečnostní předpis
Směrnice rektora č. 17/2008
Organizační řád CVIS 2018 (Vnitřní předpis č. 1/2018)
Etický kodex CVIS (pokyn)
Směrnice č. 1/2017 Zajištění řídící finanční kontroly na CVIS VUT v Brně
Pravidla provozu počítačové sítě KolejNet
Pravidla provozu sítě KolejNet pro připojení přes komerčního poskytovatele připojení
Pravidla provozu počítačové sítě VUT v Brně
Pravidla správy počítačové sítě
Pravidla provozu elektronické pošty na VUT v Brně + Dodatek
Pravidla provozu elektronické pošty sítě KolejNet
Zásady přijatelného užití sítě národního výzkumu a vzdělávání CESNET2
Prohřeškový řád sítě KolejNet
Nařízení správce sítě v aktuálním znění
Upozornění správce sítě v aktuálním znění
Směrnice IS VUT v aktuální verzi

3.3. Analýza situace

Počáteční fází řízené změny je rozhodnutí, jestli je či není nutné a vhodné provést plánovanou změnu. Rozhodujeme na základě dobře zvolených analýz a metod strategické analýzy. V závěru kapitoly nám poslouží výstupy z analýz obecného okolí a interních faktorů jako zdroje informací pro Lewinův model, který poté napomůže určit posloupnosti jednotlivých fází procesu řízené změny. Analýza oborového prostředí, jejímž cílem je zjištění stavu v daném oboru, postrádá v tomto případě smysl, neboť uživatelé mohou volit pouze mezi dvěma předdefinovanými poskytovateli připojení ve všech lokalitách oddělení. [14]

3.3.1. SMART cíle

Dalším úkolem této práce je správně nastavený cíl, případně několik cílů, které mají být naplněny tímto projektem. Ke správnému řešení mám pomůže metodika stanovování cílů SMART, doplněná o matici odpovědnosti RACI. [21]

		SPECIFICKÝ	*REÁLNÝ*	*AKCEPTOVATELNÝ*	*TERMÍNOVANÝ*	*MĚŘITELNÝ*	
	SMART	**CO ?**	**JAK ?**	**KDO ?**	**KDY ?**	**KOLIK ?**	**Sledování**
	Název cíle	*(předmět)*	*(zdroje, náklady)*	*(odpovědnosti)*	*(termíny)*	*(vyhodnocení)*	*(aktualizace)*
Hlavní cíl	**Vývoj aplikace na analýzu rizik**	zavedení ISMS, usnadnění provozu	Vlastní zdroje (lidské, SW i HW)	stanovuje RACI matice	14 dní před datumem odevzdání diplomové práce	zlepšení dostupnosti a přehlednosti dat z analýzy o 50%	zpětná vazba od pracovníků bezpečnosti
Vedlejší cíl	**Testování aplikace**	testy funkčnosti aplikace	Vlastní zdroje (lidské, SW i HW)	stanovuje RACI matice	Do 10.5. 2020	aplikace vyhodnocuje smysluplná a zálohovaná data	zpětná vazba od vývojářů a testerů
Vedlejší cíl	**Zavedení do provozu a integrace do systému**	integrace do IS a implementace do prostředí, školení	Vlastní zdroje (lidské, SW i HW)	stanovuje RACI matice	Do 31.12.2020	aplikace je provozován a v IS a obsluha je proškolena	kontrola vedoucím pracovníkem
Vedlejší cíl	**Aktualizace dat**	udržování systému i aplikace samotné	Vlastní zdroje (lidské, SW i HW)	stanovuje RACI matice	Opakovaně, každý rok do 1. 3. nebo dle potřeby	bezpečnostní incidenty eliminovány ročně o 20%	kontrola vedoucím pracovníkem

Obrázek 13: stanovení SMART cíle (Vlastní zpracování dle: [21])

	RACI MATICE ODPOVĚDNOSTI							
			ČLENOVÉ TÝMU					
	CÍLE	***vývojář***	***tester***	***obsluha aplikace***	***vedoucí areálu***	***vedoucí oddělení***	***ostatní zaměstnanci oddělení***	***ředitel útvaru***
1	**Zavedení ISMS**	**I**	**I**		**C**	**R**	**I**	**A**
2	**Vývoj aplikace**	**R**	**C**		**I**	**A**	**I**	**I**
3	**Testování aplikace**	**C**	**R**		**I**	**I**	**C**	**I**
4	**Systémová integrace**	**R**	**C**		**I**	**A**	**I**	**I**
5	**Zavedení aplikace do provozu**	**C**	**C**		**I**	**R**	**I**	**I**
6	**Školení zaměstnanců**	**R**	**C**		**I**	**A**	**I**	**I**
7	**Školení obsluhy aplikace**	**R**	**C**		**I**	**A**	**I**	**I**
8	**Aktualizace dat**	**I**	**I**	**R**	**C**	**A**	**I**	

Obrázek 14: stanovení matice odpovědnosti (Vlastní zpracování dle: [21])

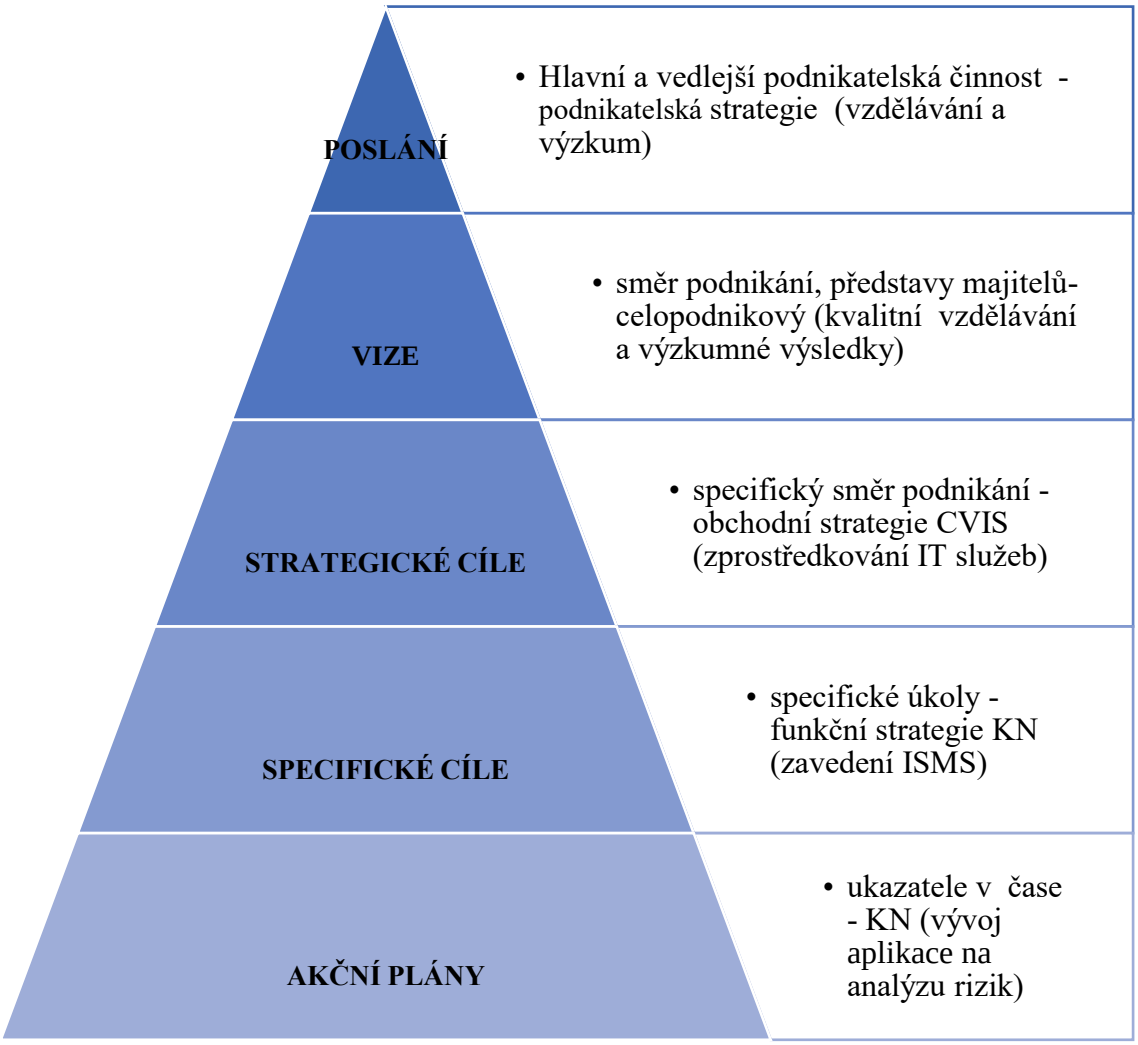
Matice odpovědnosti RACI zobrazuje čtyři druhy rolí odpovědnosti:

- R – Responsible – ten, kdo úkol vykonává,
- A – Accountable – ten, kdo úkol podepisuje čili má věcnou odpovědnost,
- C – Consulted – ten, kdo má informace, které mohou napomoct ke splnění úkolu,
- I – Informed – ten, kdo je informován o stavu úkolu. [21]

3.3.2. Hierarchie plánování

Následující diagram přehledně zobrazuje zařazení aplikace do hierarchie plánování. Obrázek nám také pomůže vizualizovat na jakou úroveň řízení aplikaci zařadit a jakým

způsobem se v otázkách týkajících se aplikace rozhodovat, případně s kým změny konzultovat.

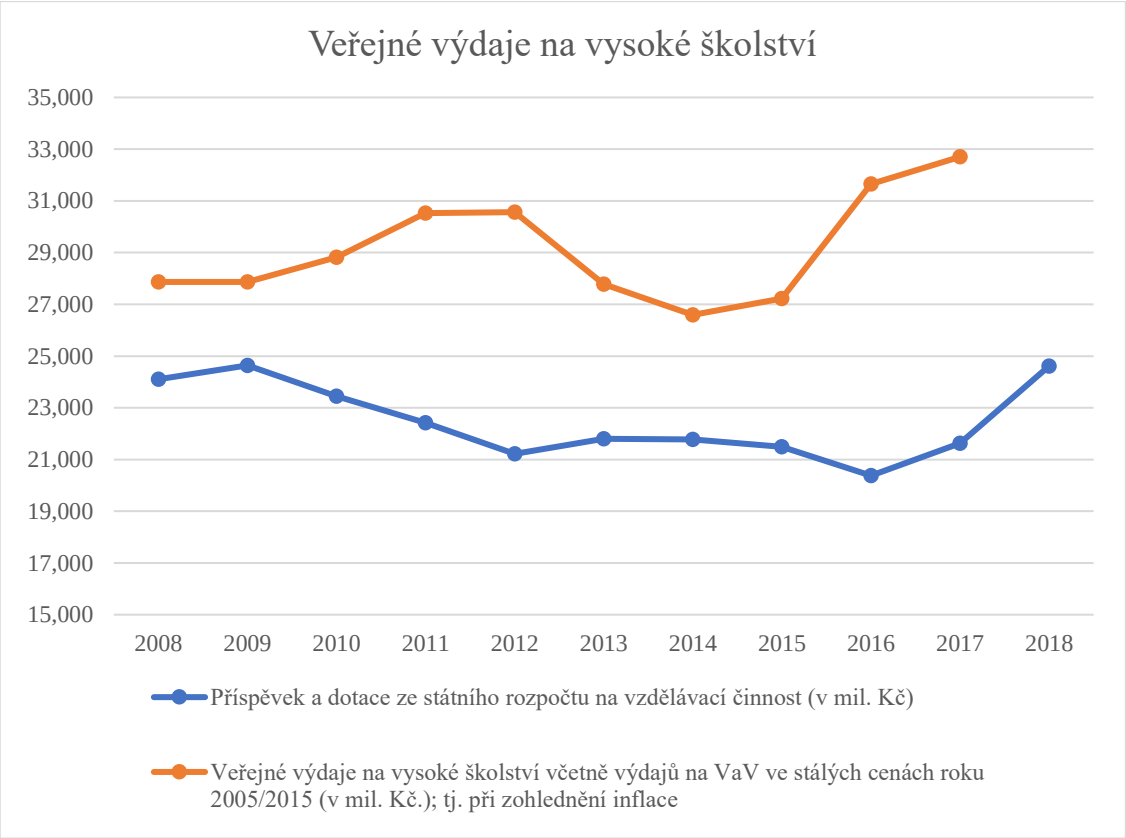


Obrázek 15: hierarchie plánování (Vlastní zpracování dle [14])

3.3.3. SLEPT analýza

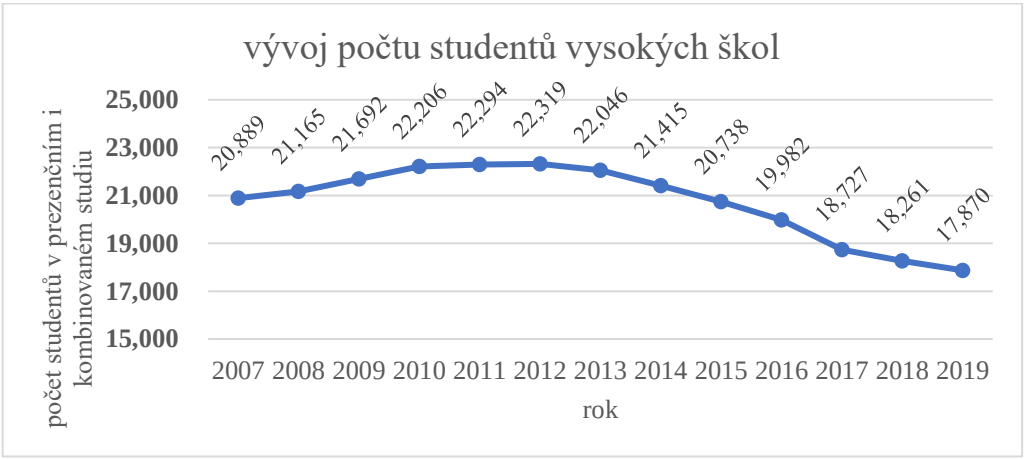
Úspěšnost naplnění cíle určuje také soulad zvolené strategie s okolním prostředím podniku. V následující analýze určíme vliv jednotlivých vnějších faktorů vycházejících z obecného okolí na zvolenou změnu a cíle oddělení. V této analýze hodnotíme jednotlivé sociální, ekonomické, politické, legislativní a technologické faktory. [14]

Jelikož je popisovaná organizace veřejnou vysokou školou, a je financována ze státního rozpočtu, je současná politická a ekonomická situace velmi podstatná pro rozhodování. Veřejné výdaje na terciální sektor školství, podle statistik ministerstva školství, mládeže a tělovýchovy, jsou uvedeny v následujícím grafu.



Graf 1: veřejné výdaje na terciální sektor školství (Zdroj: [20])

I přesto, že nenalézáme rostoucí trend v přidělování finančních prostředků vysokým školám, pozorujeme kolísání okolo velmi vysoké hodnoty. V porovnání s poklesem počtu studentů vysokých škol (viz. Graf 2) se tedy nejedná o zhoršení podmínek pro vzdělávání, ale pravděpodobně spíše o rozvážnější přerozdělování finančních zdrojů státního rozpočtu s ohledem na aktuální stav školství i ekonomiky státu. Strategická rozhodnutí by tedy měla být pečlivě zvážena a důkladně analyzována.



Graf 2: stav studentů VUT v Brně (Zdroj: [20])

Oddělení CVIS vykazuje, dle Výroční zprávy o hospodaření Vysokého učení technického v Brně za rok 2018, hospodářský výsledek z hlavní činnosti menší (20 tis. Kč), než z činnosti doplňkové (977 tis. Kč). Vzhledem k tomu, že nejsou veřejně dostupná podrobnější data, považujeme kladný hospodářský výsledek za dobrý a prostředí připravené k investicím do rozvoje nejen interního prostředí. [9]

Tabulka 5: výsledek hospodaření (v tis. Kč) jednotlivých součástí VUT za rok 2018 (Zdroj: [9])

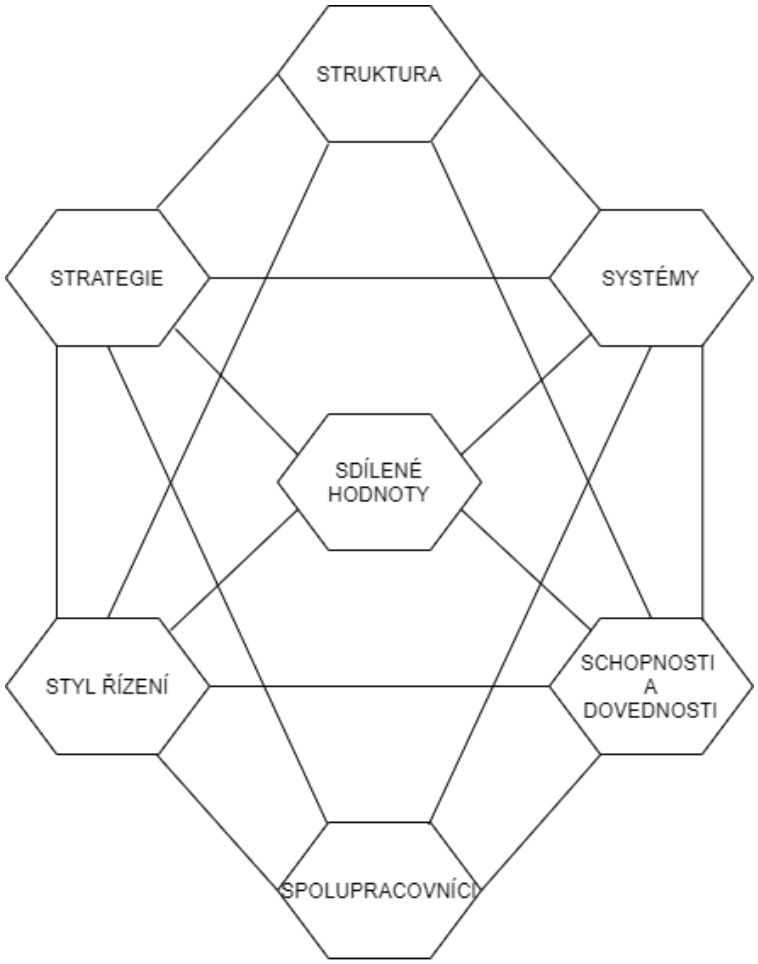
Součást VVŠ	VH z hlavní činnosti	VH z doplňkové činnosti	**VH celkem**
FAVU	382	111	**493**
FAST	3379	6419	**9798**
FSI	3380	10310	**13690**
FIT	892	3156	**4048**
FA	15	136	**151**
FCH	618	2697	**3315**
FP	475	323	**798**
FEKT	1649	5219	**6868**
CESA	74	620	**694**
ICV	1055	1	**1056**
ÚSI	842	73	**915**
STI	24	4008	**4032**
CVIS	20	977	**997**
ÚK	0	0	**0**
VUTIUM	0	642	**642**
KaM	17 885	15904	**33789**
Rektorát VUT	3095	15115	**18210**
CELKEM	33785	65711	**99496**

Technologický rozvoj v celé organizaci je na velmi dobré úrovni, nacházíme zde několik generací odborníků se znalostmi a zkušenostmi na vysoké úrovni. V provozu jsou používány nejmodernější technologie a kvalitní zařízení, infrastruktura je budována za předpokladu dalšího rozvoje. [9]

3.3.4. Model 7S

Analýza McKinsey 7S řeší kritickou otázku koordinace v organizaci, jedná se tedy o interní analýzu. Na základě zmapovaných vazeb mezi interními faktory, kde zároveň

chybí hierarchické struktury, podtrhujeme skutečnost, že změna nebo pokrok v jedné z částí organizace bude velmi složitý proces, pokud nebude řešen ve spolupráci s ostatními faktory. [13][14]



Obrázek 16: McKinsey model 7S (Vlastní zpracování dle: [13])

Nyní budeme jednotlivě zkoumat modelem zadané faktory. Zaobírat se budeme pouze hodnoceným oddělením. Prvky 7S třídíme do dvou kategorií na „tvrdé“, které snadněji určíme a ovlivníme. Příkladem je vhodná struktura a kvalitní podpůrné systémy jako podpora pro dosažení strategie. Organizační struktura oddělení je velmi jednoduchá, tvoří jej hierarchie dvou úrovní vedoucích pracovníků a jednotliví podřízení operativní pracovníci. Počet pracovníků je nízký, hovoříme o 12 zaměstnancích v jednom oddělení, pod pravomocemi nadřazeného organizačního celku. Významné rozhodovací procesy je nutno konzultovat a schvalovat právě na této, vyšší, úrovni řízení. Jedním z těchto případů je získávání a rozdělování finančních zdrojů. Větší volnost má oddělení v určování využití lidských zdrojů, často se jednotlivé pracovní náplně dají snadno delegovat na

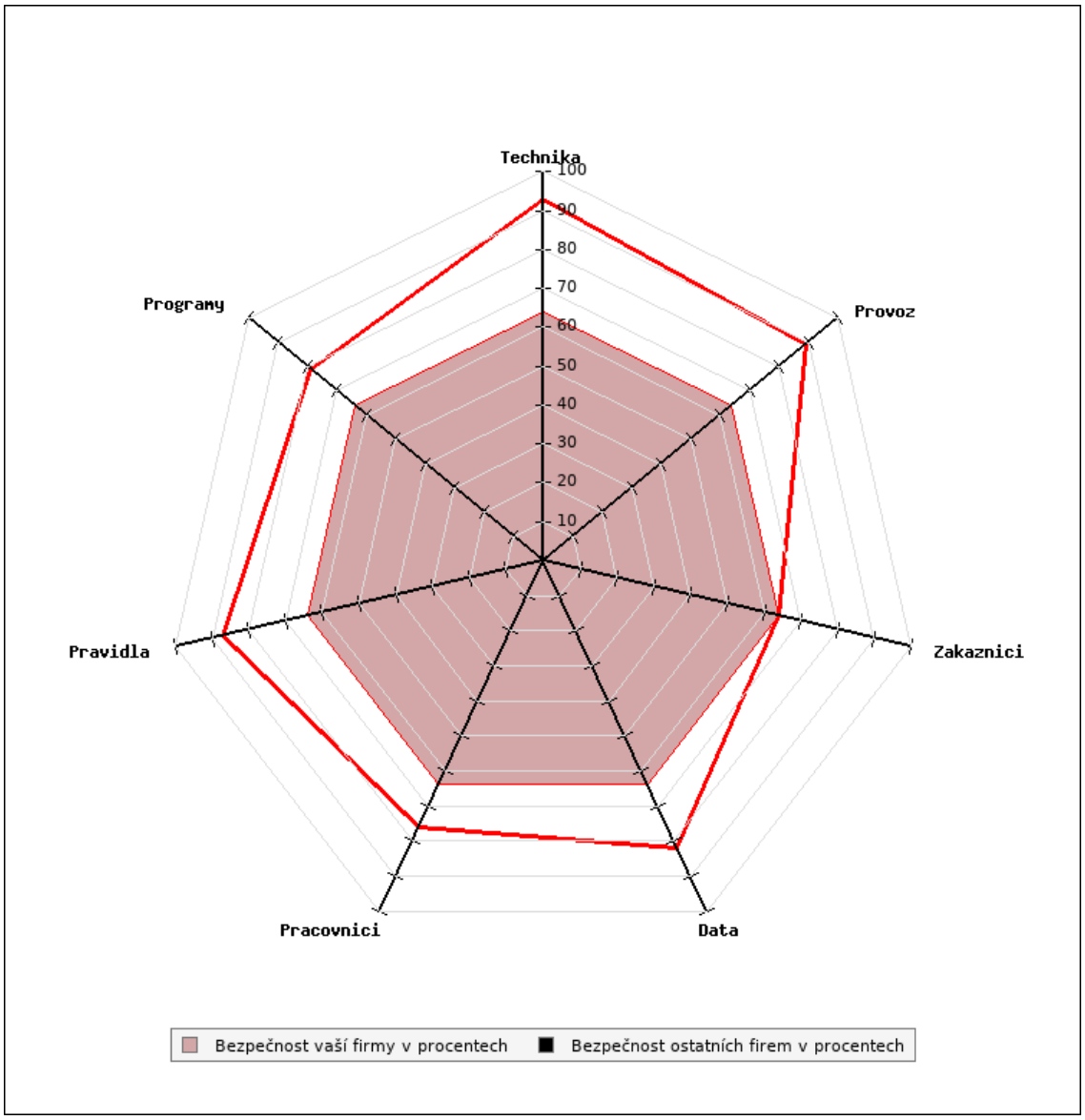
jiného pracovníka, což je z velké části umožněno odborností pracovníků. Faktor systémů v organizaci hraje velmi významnou roli, oddělení využívá informační systém, vytvořený na míru svým potřebám, v drtivé většině pracovních procesů i projektů. Takový systém se stává velmi zranitelným, a v případě jeho nefunkčnosti může dojít k finanční ztrátě.

Takzvané „měkké“ faktory, které jsou jen těžko měřitelné, tvoří vhodně řízené (motivované) lidské zdroje s vhodnými dovednostmi a schopnostmi, mající stejné sdílené hodnoty. [13] V oddělení neexistuje žádný dokument, který by ohraničoval tyto měkké dovednosti, proto nelze přesně vymezit sdílené hodnoty. V tomto případě se lze řídit opět rozhodnutími na vyšších úrovních, například etickým kodexem platným pro celou organizaci. Co lze určit s jistotou jsou schopnosti spolupracovníků, ty jsou na vysoké úrovni a jsou testovány pravidelným školením. Faktor času hraje důležitou roli při všech pracovních činnostech, některé případy vyžadují velmi krátkou dobu odezvy (řešení potíží s připojením), jiné procesy či projekty by naopak zasloužily rozšíření časové dotace. Velmi nevyváženými prvky jsou motivace a vedení. Absence projektového řízení ještě více podporuje nedostatek motivace pracovníků a definuje vedení lidských zdrojů jako strohé a neefektivní.

Z analýzy vyplývá, že je nedostatečně využíváno potenciálu zaměstnanců. Vzhledem ke své odbornosti a často i získaným zkušenostem, mohou pracovníci obohatit zásobu aktiv i hrozeb, s jimiž aplikace pracuje, o relevantní prvky, proto bude aplikace obsluhována pracovníkem. Informační systém je zde kritickou součástí celého provozu oddělení, proto je důležité udržovat jej aktuální a zabezpečený, totéž platí pro všechny součásti, které se do informačního systému integrují.

3.3.5. Hodnocení bezpečnosti v oddělení pomocí aplikace ZEFIS

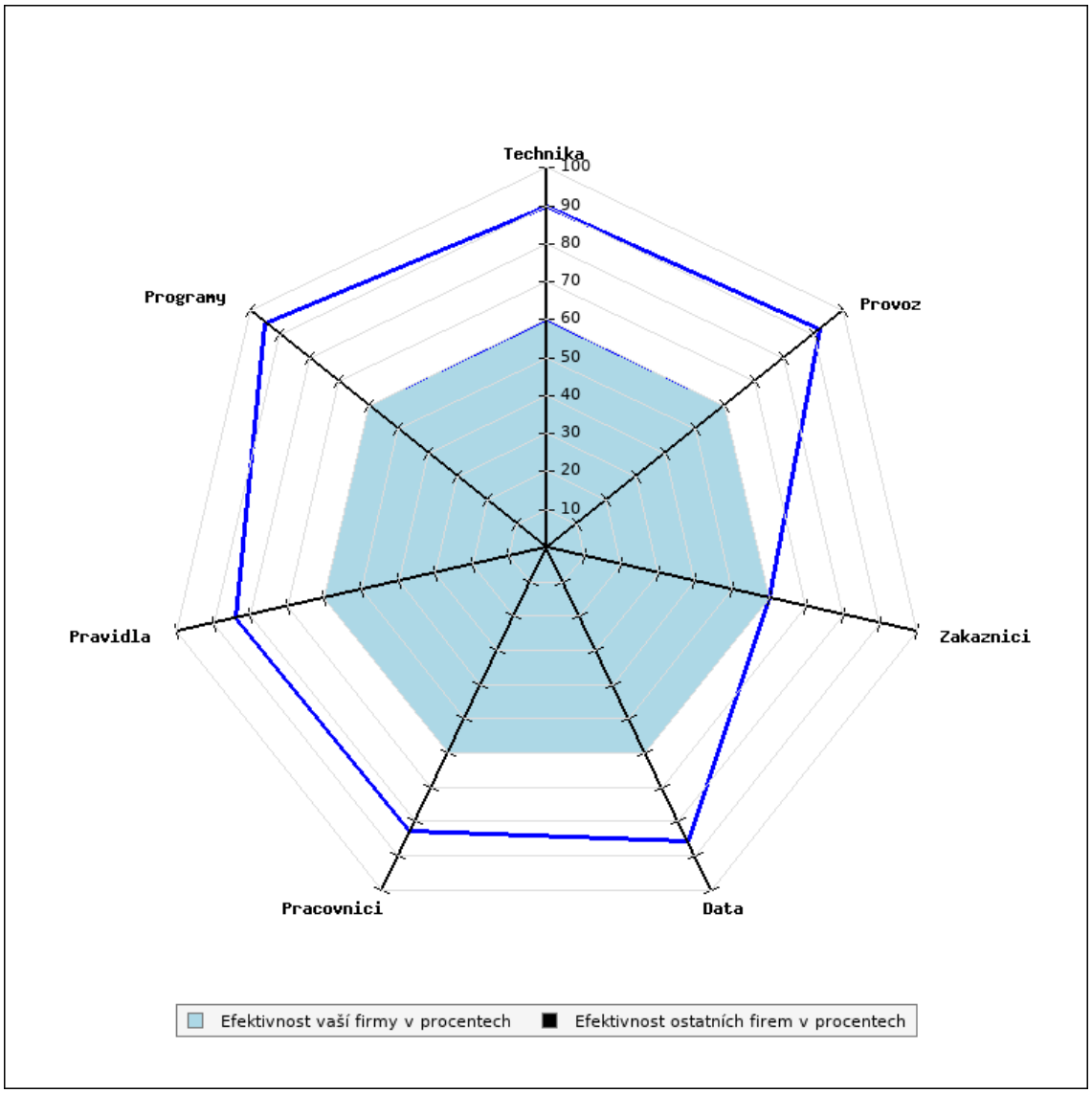
Celková bezpečnost je vždy určována nejslabším článkem celého systému. [15] V technické oblasti je na tom firma velmi dobře (93 %, to značí téměř plnou shodu s ideálním stavem bezpečnosti), obdobně vysokých hodnot dosahuje v případě oblasti nastavených pravidel a provozu či oblasti dat. Pod hranicí 80 % se nacházejí programy a pracovníci. Tyto dvě oblasti jsou na sobě plně závislé, funkčnost informačního systému i jeho doplňků závisí na vývojářích a administrátorech. Provozovat tak rozhlehlou síť bez centrálního a uzpůsobeného IS je však téměř nemožné. Nejnižší procento (64 %) má oblast zákazníků. Tato oblast je ovšem velmi těžko regulovatelná z pohledu oddělení.



Graf 3: pavučinový graf bezpečnosti v oddělení (Zdroj: [15])

3.3.6. Efektivita IS a procesů

Abychom naplnily stanovené cíle, potřebujeme správně vybrané, nastavené a provozované informační systémy a procesy, bez nedostatků a chyb. [15] Celková efektivnost je 60 %, a je tedy nižší než celková bezpečnost. Hodnoty jednotlivých oblastí se pohybují v intervalu 60 % až 95 %, a jsou poměrně vysoké. Nejvyšší efektivitu mají právě programy, a to zejména proto, že jsou šité na míru potřebám oddělení. Nejnižších 60 % dosahují zákazníci, tuto oblast lze částečně omezovat či směrovat pravidly či nařízeními, u jejich dodržování je ale složité provádět kontrolu.



Graf 4: efektivita IS a procesů (Zdroj: [15])

3.3.7. Nedostatky

Systém ZEFIS dále vyhodnotil několik nedostatků v několika oblastech při hodnocení využití IS v oddělení.

Vysokou významnost přidělil ZEFIS nedostatkům v těchto oblastech:

Tabulka 6: významné nedostatky IS oddělení (Zdroj: [15])

Oblast	Významnost	Bezpečnost	Typ	Název
Pracovníci	Vysoká	Ano	Neshoda	Nedodržování pravidel
Pravidla	Vysoká	Ne	Neshoda	Chybí informační strategie

Tyto dva výstupy spolu navzájem souvisí, můžeme předpokládat, že vytvoříme-li pro oddělení dokumentovanou informační strategii (spolu se zavedením ISO/IEC 27 000), která je smysluplná a zasahuje do všech potřebných oblastí, můžeme tím částečně zabránit nechuti pracovníků dodržovat pravidla.

Střední a nízkou významnost přidělil ZEFIS nedostatkům v těchto oblastech:

Tabulka 7: středně a slabě významné nedostatky IS oddělení (Zdroj: [15])

Oblast	Významnost	Bezpečnost	Typ	Název
Pravidla	Střední	Ano	Neshoda	Chybějící, nebo špatně dodržovaná bezpečnostní pravidla
Technika	Nízká	Ne	Neshoda	Riziko zbytečných nákladů z nekompatibilní techniky

Tato tabulka opět zobrazuje problém s pravidly v organizaci, pro tuto sekci jsme již zavedli opatření, zavedením ISO/IEC 27 000. Součástí tohoto systému bude také již zmíněná aplikace, kterou integrujeme do informačního systému. Oblast techniky s nízkou významností poukazuje na důležitost správného výběru zařízení pro připojení do sítě, tato zařízení musí být kompatibilní a spolehlivá, jinak vznikají zbytečné vícenáklady.

3.3.8. Analýza rizik projektu

Hranice analýzy rizik projektu určíme po sestavení seznamu aktiv. Aktiva, která mají vztah k cílům projektu zahrneme, ostatní aktiva, po důkladném uvážení, nezahrneme. [14]

ANALÝZA RIZIK

1. IDENTIFIKACE AKTIV

Aktivum	Primární/Podpůrná	Druh	Garant				Ohodnocení z pohledu:		Klíčové aktivum
název	Kategorie			Důvěrnos	Dostupn	Integrita	Hodnota	Dopad	
infrastruktura	**Primární**	HW	Vedoucí	5	5	5	5	6	ANO
ISMS	**Podpůrné**	Systém řízení	Vedoucí, Správce	4	5	4	4	4	NE
webová aplikace	**Podpůrné**	SW	Vedoucí, Správce	4	3	5	4	4	NE
osobní údaje zákazníků	**Podpůrné**	INF	Vedoucí	5	4	5	5	7	ANO
různá jiná data oddělení	**Podpůrné**	INF	Vedoucí	4	4	5	4	4	NE
elektronické nosiče (CD, flash disk)	**Podpůrné**	HW	Vedoucí	3	2	3	3	5	NE
ostatní nosiče (papír. dokumentace)	**Podpůrné**	HW	Vedoucí	2	2	2	2	2	NE
vnitřní směrnice a postupy	**Podpůrné**	INF	Vedoucí	5	4	5	5	6	ANO
Informační systém	**Primární**	SW	Vedoucí	5	5	5	5	7	ANO
kvalifikace personálu	**Primární**	Lidská	Zaměstnanec	5	5	4	5	5	ANO
autorská práva	**Primární**	Lidská	Vedoucí	3	3	4	3	4	NE
pracovní morálka	**Primární**	Lidská	Zaměstnanec	3	3	4	3	7	ANO

Obrázek 17: identifikovaná aktiva se vztahem k projektu (Vlastní zpracování)

Předchozí seznam je redukovaný výběr ze všech aktiv organizace, tyto aktiva mají vztah k cílům projektu, a proto je zahrneme do analýzy rizik. Hodnocení bylo provedeno podle kritérií uvedených v příloze č. 1. Klíčová aktiva jsou ta nejkritičtější aktiva v oddělení. V další tabulce ohodnotíme dopad hrozeb na aktiva.

aktivum			*webová aplikace*	*osobní údaje zákazníků*	*různá jiná data oddělení*	*elektronické nosiče (CD, flash disk)*	*ostatní nosiče (papír. dokumentace)*	*vnitřní směrnice a postupy*	*Informační systém*	*kvalifikace personálu*	*autorská práva*	*pracovní morálka*	*infrastruktura*	*ISMS*
Hrozba	**děpodob**	**Hodnota**	**Hodnota dopadu na aktiva**											
požár	Střední	2	3	4	2	1	1	3	5	x	2	x	5	3
nedostatek času/ překroč. čas. plánu	Velká	3	3	1	1	1	1	3	3	4	3	3	1	5
závažná nehoda	Malá	1	5	4	3	2	1	3	5	4	3	4	5	4
zničení zařízení nebo medií	Malá	1	5	4	3	5	5	3	5	x	x	x	5	3
chyba lidského faktoru	Velká	3	4	4	2	1	1	4	5	4	3	4	5	4
nedostatek finančních zdrojů	Střední	2	3	2	1	1	1	2	5	5	2	4	3	5
nedostatek motivace	Malá	1	4	2	2	1	1	3	4	5	3	5	3	4
znepřístupnění dat (hacker, cracker…)	Malá	1	5	5	3	3	3	4	5	x	5	x	5	2
odposlech a vyzrazení	Malá	1	4	5	2	2	2	5	5	x	4	x	5	3
falšování dat	Malá	1	5	5	3	4	4	5	5	3	5	5	5	3
změna právního řádu	Střední	2	3	5	3	2	2	4	4	4	4	4	3	4
aktualizace normy	Střední	2	4	1	3	3	3	4	3	5	2	5	3	5

Obrázek 18: hodnocení hrozeb a jejich dopadu na aktiva (Vlastní zpracování)

Některé jmenované hrozby představují pro projekt významná rizika, tato významnost bude posouzena v dalším kroku analýzy. Tabulka hodnocení dopadu hrozeb na aktiva je k nalezení opět v příloze č. 1.

	aktiva	*webová aplikace*	*osobní údaje zákazníků*	*různá jiná data oddělení*	*elektronické nosiče (CD, flash disk)*	*ostatní nosiče (papír. dokumentace)*	*vnitřní směrnice a postupy*	*Informační systém*	*kvalifikace personálu*	*autorská práva*	*pracovní morálka*	*infrastruktura*	*ISMS*
Hrozba	RIZIKO	SW	INF	INF	HW	HW	INF	SW	Lidsk	Lidsk	Lidsk	HW	Systém řízení
požár		6	8	4	2	2	6	10	#	4	#	10	6
nedostatek času/ překroč. čas. plánu		9	3	3	3	3	9	9	12	9	9	3	15
závažná nehoda		5	4	3	2	1	3	5	4	3	4	5	4
zničení zařízení nebo medií		5	4	3	5	5	3	5	#	#	#	5	3
chyba lidského faktoru		12	12	6	3	3	12	15	12	9	12	15	12
nedostatek finančních zdrojů		6	4	2	2	2	4	10	10	4	8	6	10
nedostatek motivace		4	2	2	1	1	3	4	5	3	5	3	4
znepřístupnění dat (hacker, cracker…)		5	5	3	3	3	4	5	# #	5	# #	5	2
odposlech a vyzrazení		4	5	2	2	2	5	5	#	4	#	5	3
falšování dat		5	5	3	4	4	5	5	3	5	5	5	3
změna právního řádu		6	10	6	4	4	8	8	8	8	8	6	8
aktualizace normy		8	2	6	6	6	8	6	10	4	10	6	10

Obrázek 19: vyhodnocení úrovně rizika (Vlastní zpracování)

Pro vyhodnocení je použita metoda se dvěma parametry, a následující výpočet:

$$R = hodnota\ pravděpodobnosti\ vzniku\ hrozby * hodnota\ dopadu\ hrozby$$

Výsledné hodnoty větší jak 7 považujeme za vysoká rizika a jsou označeny červeně, rizika s hodnocením 6, vyžadují taktéž naši pozornost, nejsou ovšem tak závažná. Nejlepšími způsoby rozpoznání rizika je kontrola seznamu úkolů a časového plánu a diskuse a rozhovory s odborníky. Přijatelné náklady na zpoždění jsou stanoveny maximálně na 20 000 Kč, vyšší náklady představují velkou finanční zátěž oddělení. [14]

3.3.9. Lewinův model

Lewinův model napodobuje jednotlivé fáze procesu řízené změny v podniku. Tento model sestavíme pro proces vývoje a nasazení aplikace do oddělení. Výsledkem je nevyhovující současný stav, rychlý rozvoj technologií sebou přináší i možnosti existence významných hrozeb a vytváří tak nová a nová podnikatelská rizika. Na základě předchozích analýz vnějšího i vnitřního prostředí bylo rozhodnuto o zahájení projektu vývoje a implementace aplikace, a nyní je vhodné správně určit jednotlivé informace o změně samotné. [14]

Za inicializační faktor můžeme označit nárůst bezpečnostních incidentů v oddělení, které mají různě velký vliv na správný provoz počítačové sítě. Ty velmi významné bezpečnostní incidenty mohou úplně přerušit hlavní činnost oddělení a způsobit finanční ztráty nebo vyřadit některá zařízení z provozu. [14]

Požadovaný budoucí stav oddělení, kterého chceme dosáhnout je efektivní využívání aplikace na analýzu rizik ke snížení počtu bezpečnostních incidentů, snížení rizik a případné snížení nákladů na obnovu dotčených prvků do běžného provozu.

Proces vývoje a provozu aplikace by měl být podporován zejména vedením, taková podpora zajistí přidělení potřebných zdrojů. Aby byla efektivita aplikace maximalizována, měli by její provoz podporovat všichni zaměstnanci a poskytovat zpětnou vazbu. V tomto případě je agentem změny neboli nositelem procesu změny ve firmě, skupina zaměstnanců, podílejících se na vývoji a testování aplikace. Sponzorem změny je další součást nadřazená v organizační struktuře. [14]

Téměř ve všech oblastech bude proveden určitý stupeň intervence. Nejvíce bude ovlivněn IS a také lidské zdroje a jejich řízení, naproti tomu technologie používané v oddělení

budou pravděpodobně ovlivněny minimálně. Do organizace přibydou se zavedením ISMS i provozem aplikace nové procesy a komunikační toky. Celý vývoj a provoz je veden jako projekt, proto musíme naplnit všechny tři hlavní fáze projektu, vlastní změna tak dostane určitý řád. V předprojektové fázi připravujeme podmínky pro realizaci změny, projektová fáze přestavuje provedení změny a v poslední fázi má agent změny za úkol zamrazit požadovaný stav, a je vhodné také zhodnotit dosažené výsledky. [14]

3.3.10. Zavedení ISMS

Při zavádění Systému managementu bezpečnosti informací (zkr. ISMS) podle řady norem ČSN ISO/IEC 27 000, a především při jeho udržování, využije oddělení jednoduchou webovou aplikaci na analyzování bezpečnostních rizik. Pro řízení rizik existuje v této řadě norem speciální část, ČSN ISO/IEC 27 005, která se zaměřuje právě na tuto problematiku. Webová aplikace bude zařazena do dokumentu Bezpečnostní politika, který je vytvářen při zavádění kompletního ISMS do organizace. Taktéž bude pro obsluhu této aplikace vytvořen návod v dokumentované podobě, ve formě vnitřní směrnice. Normy dále kladou důraz na udržování, kontrolu a aktualizaci celého ISMS a všech jeho součástí, obecně tento proces shrnuje Demingův PDCA diagram. Podle tohoto cyklu bude probíhat také údržba, provoz a aktualizace webové aplikace. [6]

3.4. Webová aplikace

Aplikace na analýzu rizik bude vytvořena pomocí programovacího jazyka HyperText Markup Language (HTML) a dynamické prvky budou programovány pomocí jazyka Javascript a PHP, bude tedy dostupná z webového rozhraní. Tento způsob vývoje byl zvolen především proto, že informační systém, přístupný z webového rozhraní, slouží pro centrální správu, a tato webová aplikace bude jednoduše zařazena mezi prvky správy a jeho zdrojové kódy umístěny na serveru.

3.4.1. SWOT analýza využití aplikace

Před zahájením vývoje provedeme analýzu silných a slabých stránek využití této aplikace, abychom zjistili, zda bude tato aplikace pro oddělení KolejNet prospěšná a nebude pouze zbytečně vytěžovat finanční zdroje oddělení. V této analýze jsou sumarizovány dílčí závěry z předchozích analýz. Analýzu zpracujeme v tabulkovém procesoru Excel, kdy do

řádků budeme určovat jednotlivé prvky silných a slabých stránek a příležitostí a hrozeb. Tyto prvky následně ohodnotíme váhou (určující závažnost faktoru vůči analyzované aplikaci), kterou představuje číselná hodnota z rozsahu 1 až 10, kde hodnota 10 určuje nejzávaznější faktor. Dále spočteme sumu vah pro jednotlivé kategorie faktorů samostatně. Sumu vah slabých stránek odečteme od sumy vah silných stránek $(S - W)$, výsledek představuje předpoklady k naplnění cíle, směřující z vnitřního prostředí. Součet vah hrozeb odečteme od součtu vah příležitostí $(O - P)$, tento rozdíl představuje předpoklady k naplnění cíle směřující z vnějšího prostředí. Za výslednou hodnotu považujeme hodnotu rozdílu $(S - W) - (O - P)$. Silné stránky převažují nad slabými stránkami a příležitosti převažují nad hrozbami. Z analýzy vyplývá, že vnější i vnitřní prostředí je připraveno pro zavedení aplikace. Kladná výsledná hodnota značí, že provoz aplikace má pro oddělení smysl, a spuštění vývoje nic nebrání, naopak je všemi faktory podporován. [14] [16]

S - silné stránky	**váha**	**W - slabé stránky**	**váha**	**O - příležitosti**	**váha**	**T - hrozba**	**váha**
Zabezpečený přístup z informačního systému	8	Náklady na vývoj a implementaci	5	Zjednodušení auditování a logování	7	Přidružená databáze obsahuje citlivá data a informace o oddělení	7
Vizualizace a přehlednost analýzy	9	Nutné zaškolení zaměstnanců	9	Možnost rychlé změny a úprav aplikace	9	Změna organizační struktury může změnit pracovní pozici pro obsluhu aplikace	4
Jednoduchá správa historických dat i informací	10	Potřeba aktualizace dat ve stanoveném intervalu	4	Změna sídla organizace výrazně neovlivní množinu výchozích aktiv.	5	Provoz aplikace bez existujícího systému řízení rizik či bez celopodnikových pravidel	5
Nízké náklady na provoz, bez nutnosti fyzického skladování dokumentů	8	Pouze částečná automatizace, nutnost obsluhy	4	Možnost integrace aplikace do dalších oddělení nebo systémů organizace	8	Provoz závislý na centrálním informačním systému	8
Jednoduché zálohování a obnovení dat	7	Potřeba zavedení systému řízení rizik	5	Možnost rozvoje aplikace do vetších celků	6	Nedostatek kvalifikovaných zaměstnanců a špatné experní odhady	5
součet vah	42	**součet vah**	27	**součet vah**	35	**součet vah**	29
hodnocení S - W	15			**hodnocení O - T**	6		
Celkové skóre (S - W) - (O - T)		**9**					

Obrázek 20: SWOT analýza využití aplikace (Vlastní zpracování dle: [14][16])

4. VLASTNÍ NÁVRH ŘEŠENÍ

Vlastní návrh řešení představuje návrhy autora k řešení problematiky diplomové práce, tedy k vytvoření webové aplikace na analýzu rizik. Tato aplikace je sice zasazena do již existujícího prostředí, její variabilita a jednoduchost však umožňuje její využití i jinde, a to jako součást systému řízení bezpečnosti informací nebo samostatně.

4.1. Stanovení kontextu

Tato podkapitola obsahuje vymezení základních kritérií pro analyzování rizik v oddělení, definice rozsahu a hranic, a stanovení organizační struktury pro analýzu rizik. Pomyslná hranice oddělení v organizační struktuře CVIS poslouží i jako hranice rozsahu platnosti webové aplikace pro analyzování rizik. Tuto hranici lze překročit v případě, že se mimo oddělení vyskytují externí hrozby, které by se mohly do sítě KolejNet rozšířit. Jako příklad můžeme uvést informační službu tzv. CERT/CSRIT (Computer Emergency Response Team/Computer Security Incident Response Team) bezpečnostních týmů uznaných úřadem Trusted Introducer, které zajišťují přecházení vzniku bezpečnostních incidentů vzniklých v počítačových sítích, koordinují jejich řešení a informují o tomto řešení. Oddělení získává užitečné informace od oficiálních týmů spolupracujících v e-infrastruktuře CESNET (CESNET-CERT, CSIRT-MU a CSIRT-VUT) elektronickou poštou. [10]

4.2. Aktiva

Za aktiva považujeme všechen hmotný i nehmotný majetek v organizaci. V průběhu sběru dat a pragmatické analýzy se aktiva vytřídí na ty, která budou použita pro analýzu a na ostatní aktiva. Tato množina aktiv bude rozdělena na primární a podpůrná aktiva. Primární aktiva můžeme také označit jako jedinečné, složitě nahraditelné aktivum, jehož hodnotu posuzujeme podle velikosti škody způsobené zničením či ztrátou aktiva. [1][14]

4.2.1. Identifikace aktiv

Aktiva je vhodné identifikovat ve stanoveném rozsahu metodou expertního odhadu nebo pomocí týmového brainstormingu. Sestavíme soupis aktiv, které leží uvnitř stanovených hranic analýzy rizik. [14]

4.2.2. Logické seskupení aktiv

Logické seskupení potom znamená, že jednotlivá aktiva kategorizujeme a seskupíme, podle toho, jestli spolu logicky souvisí a definujeme, zda se jedná o primární či podpůrná aktiva. Aktiva rozdělíme na několik kategorií, podle kterých bude probíhat také jejich ohodnocení. Mezi hardware a software řadíme prvky infrastruktury, aktivní prvky a jejich softwarové vybavení. Lokalita označuje nehmotný majetek spojený s provozem oddělení. Lidská a informační aktiva pak zahrnují zaměstnance a jejich znalosti a zkušenosti, data a mimo jiné také dokumentované předpisy, pokyny a směrnice. [6]

4.2.3. Identifikace a evidence garantů aktiv

Za garanta neboli vlastníka aktiva považujeme osobu, která za aktivum v organizaci zodpovídá. Stejně tak je tato odpovědnost platná během bezpečnostního incidentu. [6] V našem případě se můžeme potkat pouze s několika málo druhy garantů aktiv. V největší míře představuje garanta vedoucí oddělení, ojediněle jsou pak za určitá aktiva odpovědní zaměstnanci na jednotlivých pozicích anebo zákazníci.

4.2.4. Definice stupnice a hodnotících kritérií

V této kapitole definujeme hodnotící stupnice a hodnotící kritéria pro hodnocení aktiv. Při jejich stanovení bereme v potaz různé faktory. Jedním z faktorů hodnocení je velikost oddělení, i přes malý počet zaměstnanců, spravuje oddělení velké množství dat a má rozsáhlou komunikační infrastrukturu. Některá zpracovávaná data mají charakter osobních údajů (IP adresa, jméno a příjmení atd.), ale žádná z těchto dat nejsou citlivé osobní údaje, i tak se v některých případech uvažuje při hodnocení také dopad na uživatele nebo zaměstnance samotné. V některých případech může rozhodovat rozsah narušení vnitřních řídících a kontrolních činností v oddělení.

4.2.5. Ohodnocení aktiv

Jednotlivá aktiva, hodnotíme z hlediska integrity, důvěrnosti a dostupnosti. Hodnocení důvěrnosti, dostupnosti a integrity provádíme podle stanovené stupnice upřesněné v hodnotících tabulkách. Expertním odhadem pověříme osobu, jenž má přehled v daných hodnocených oblastech, případně vytvoříme tým vhodných osob a provedeme

brainstorming. Výsledná hodnota je pak aritmetickým průměrem tří vypsaných hodnot. [6]

$$hodnota\ aktiva = \frac{důvěrnost + dostupnost + integrita}{3}$$

Další důležitý, kvantitativně vyjádřený znak aktiva, je velikost dopadu na oddělení při jeho ztrátě, porušení nebo zničení. Tuto hodnotu opět určuje pověřená osoba/osoby expertním odhadem a její velikost je ohraničena stupnicí. V případě lidských zdrojů uvažujeme o jejich ztrátě, to si lze představit například jako přechod kvalifikovaného zaměstnance za lepší pracovní nabídkou nebo náklady na školení.

Zjištěné hodnoty aktiv a jejich přidružené určené dopady individuálně sečteme a hodnoty porovnáme oproti hodnotě 10, která rozdělí aktiva na dvě úrovně z pohledu významnosti aktiva pro oddělení. Podpůrná aktiva, u kterých je součet menší než 10, jsou méně významná než aktiva primární. V následujících krocích bychom na tento fakt měli brát zřetel, a to zejména při nasazování opatření. V některých případech lze podpůrná aktiva vynechat z dalšího analyzování (jsou-li všechny zjištěné hodnoty velmi nízké), v tomto případě však tento postup uplatněn nebude u žádného z aktiv, neboť mezi všemi existují vazby a závislosti.

Vazby nalézáme nejvíce u hardwarových a softwarových aktiv, programové vybavení není možné provozovat bez infrastruktury. Dodavatelské řešení by značně komplikovalo provoz sítě, a proto je hardware vlastní. To dále souvisí s informačními aktivy, neboť poskytované služby jsou řízeny dokumentovanými pravidly, opět v návaznosti na uživatele a zaměstnance, kteří se těmito pravidly řídí. U každého jednotlivého aktiva pak nalézáme požadavek, aby bylo dostatečně zabezpečeno, tím zajistíme bezpečnost celého systému.

4.2.6. Další činnosti ISMS spojené s aktivy

V rámci systému řízení bezpečnosti informací existují ještě další činnosti spojené s aktivy společnosti. Tyto činnosti by měly být dokumentované a samotná aplikace je již neřeší. Během první z těchto činností stanovujeme a zavádíme pravidla ochrany nutná pro zabezpečení jednotlivých úrovní aktiv. Poté, dle úrovně aktiv, stanovíme způsoby používání aktiv a pravidla pro jejich manipulaci, a také pravidla pro bezpečné elektronické sdílení aktiv nebo jejich fyzické přenášení. Další krok je určení způsobu

likvidace dat, provozních údajů a informací na různých typech nosičů. Těmto krokům předchází stanovení klasifikace dat (rozdělení podle stupně důvěrnosti) a klasifikace dokumentů. [6]

4.3. Bezpečnostní hrozby

Hrozba představuje událost ohrožující bezpečnost a zranitelnost slabé místo aktiva, které může být touto hrozbou využito k vytvoření bezpečnostního incidentu. Z tohoto důvodu je správnost všech částí analýzy a dobré pochopení možností vzniku hrozby zcela zásadní pro omezení působení hrozeb na oddělení. V této kapitole se opět setkáváme s několika kroky, které korespondují s kroky ISMS. [1]

4.3.1. Identifikace hrozeb a zranitelností

Identifikace relevantních hrozeb a zranitelností s ohledem na aktiva organizace je první činnost, kterou provedeme v této části. Sepíšeme seznam na základě expertního odhadu a se seznamem dále pracujeme při dalších činnostech. [6]

4.3.2. Rozdělení hrozeb a zranitelností do kategorií

Rozdělení identifikovaných hrozeb a zranitelností do kategorií umožňuje podrobnější vyhodnocení. Po vyhodnocení rizik dokážeme rozpoznat nejen nejkritičtější aktiva ale také ty nejvíce kritické oblasti hrozeb a zranitelností. Eliminaci rizika v identifikovaných oblastech pak lze provést na obou úrovních, a použít o mnoho účinnější kombinaci opatření. Během pragmatické analýzy, kdy byly použity hrozby definované v normě ISO/IEC 27 005 jako základní databáze hrozeb a zranitelností podle tzv. nejlepších zkušeností (viz. příloha 1), vykrystalizovalo několik kategorií jako technická selhání, selhání lidského faktoru, enviromentální a fyzické hrozby, neoprávněné činnosti a další. Tyto kategorie mohou být snadno rozšířeny o nové, podle potřeb oddělení.

4.3.3. Posouzení hrozeb a zranitelností

Provádění hodnocení hrozeb a zranitelností v pravidelných intervalech, nebo při významných změnách. Při hodnocení nejprve slovně hodnotíme možnost vzniku incidentu, opět podle stanovené stupnice expertním odhadem, ve třech možných hodnotách – malá pravděpodobnost, střední nebo velká pravděpodobnost. Následně

aplikace automaticky doplní kvantitativní hodnotu pravděpodobnosti vzniku hrozby, se kterou budeme dále provádět výpočty. Dopady na organizaci doplňujeme do aplikace v dalším kroku. [6]

4.3.4. Pravděpodobnost vzniku incidentu (PI)

Slovní vyjádření pravděpodobnosti je zvoleno především proto, že se hodnoty obsluze aplikace lépe odhadují. Aplikace pak hodnoty automaticky převede na číselné vyjádření pro potřeby dalších výpočtů. Pracujeme s celými čísly 1, 2 a 3, přestože mluvíme-li o pravděpodobnosti v matematice, neměly by její hodnoty přesahovat číslo 1. Pro upřesnění uvádím tabulku s procentním vyjádřením veličiny PI, nové hodnoty lze určit expertním odhadem, případně přepočtem z historických dat.

Tabulka 8: různě vyjádřená pravděpodobnost vzniku incidentu pro usnadnění výpočtu či odhadu (Vlastní zpracování)

slovní vyjádření	číselné vyjádření	procentní rozsah
malá pravděpodobnost	1	0 % - 33 %
střední pravděpodobnost	2	34 % - 67 %
velká pravděpodobnost	3	68 % - 100 %

4.3.5. Dopady na organizaci (D)

Dopady na organizaci představují hodnotu možné ztráty či poškození, vzniklé působením hrozby na aktivum, obdobně jako při analýze aktiv. Obsluha vyplňuje vždy příslušné pole samostatně do vytvořené tabulky. I přesto, že je seznam aktiv a hrozeb rozsáhlý, nelze vyhodnocovat dopady po skupinách, musíme vždy uvažovat jednotlivé aktivum vůči jednotlivé hrozbě.

4.3.6. Zpracování zprávy o hodnocení hrozeb a zranitelností

Výstupem z analýzy hrozeb a zranitelností se podle normy stává tzv. Zpráva o hodnocení hrozeb a zranitelností, sloužící jako záznam o aktuálním stavu bezpečnosti v této části. Podkladem pro její vypracování tvoří data z aplikace, ve kterých se lze přehledně orientovat a lze je také tlačítkem vytisknout. Zprávu tvoří pracovník bezpečnosti a je projednávána vedením.

4.4. Rizika

Tato kapitola obsahuje dvě rozdílné součásti. Část první obsahuje postup pro výpočet rizika a stanovení kritérií pro akceptaci neboli postoupení rizika, tyto kapitoly jsou pro webovou aplikaci velmi podstatné, a proto jim bude věnována větší pozornost. Další kapitoly pak dále doplňují obecný postup činností při ISMS, který již aplikace neřeší a vyžadují důkladné přezkoumávání pracovníky bezpečnosti informací v oddělení.

4.4.1. Obecný postup analýzy rizika

Pro výpočet hodnoty rizika je použita metoda se dvěma získanými parametry (PI a D), které se mezi sebou násobí. Postup získání hodnoty rizika je tedy následující:

- Vyhodnotíme pravděpodobnosti vzniku incidentu (PI) a jejich dopady (D), kdy veličina dopad využívá stejná hodnotící kritéria, jako aktiva.
- Vypočteme míru (intenzitu) rizika pomocí jednoduchého vztahu:

$$riziko = pravděpodobnost\ vzniku\ incidentu * dopad\ incidentu$$

- Podle velikosti získaných hodnot definujeme prioritu pro každé z rizik a tím také definujeme, jak budeme s rizikem dále pracovat a jak silná opatření budeme využívat k eliminaci rizika.
- Pro jednotlivá rizika vybereme a nasadíme opatření ke zmírnění nebo úplnému odstranění rizika, či využijeme další ze strategií snižování rizik (přenesení rizika, postoupení rizika atd). [14]

4.4.2. Kritéria pro akceptovatelnost rizik

Nasazování opatření zaváděním strategií ke snižování rizika je obvykle časově, finančně či jinak, velmi náročné. Proto je vhodné určit, kdy je riziko akceptovatelné a nebudou na něj aplikována žádná opatření. Stanovení kritérií pro akceptovatelnost rizik určuje vedoucí, jakožto osoba, která dokáže objektivně posoudit, zda je míra rizika pro oddělení únosná a zda vazby na akceptované riziko nemohou vyvolat vznik dalších rizik s vyšší prioritou. [6]

4.4.3. Výběr opatření

Na základě priorit u jednotlivých aktiv vybereme vhodná opatření a aplikujeme je na rizika. Platí pravidlo, že kombinace opatření je účinnější než použití jednoho opatření k redukci, postoupení, vyvarování se nebo přenosu rizik. Tuto oblast opět řeší pracovníci bezpečnosti a je mimo rozsah webové aplikace, nicméně bez tohoto kroku by použití ISMS téměř ztratilo význam. [1]

4.4.4. Zpracování prohlášení o aplikovatelnosti

Zpracování prohlášení o aplikovatelnosti, jakožto výstupního dokumentu komplexní analýzy s obsahem bezpečnostních opatření, která byla aplikována (včetně způsobu plnění) a která aplikována nebyla (včetně odůvodnění), provádí pracovníci bezpečnosti a schvaluje vedoucí nebo bezpečnostní výbor, v případě že je stanoven. [6]

4.4.5. Zpracování plánu zvládání rizik

Plán zvládání rizik je jedním z požadavků normy ISO/IEC 27 001, který při provozování ISMS musíme formalizovat, a to s ohledem na požadované cíle celého systému řízení rizik. Vymezuje nejčastěji odpovědnosti, přidružené činnosti vedení, potřebné zdroje a postupy při zvládání rizik dle priorit oddělení. Po formulaci Plánu zvládání rizik uvažujeme znovu nad prvky, které by mohly zavedení tohoto plánu omezit, tedy přidělené finanční zdroje, definované odpovědnosti a pravomoci, zavedená bezpečnostní opatření a také následné monitorování a přezkoumávání efektivity nastavených opatření. [6]

4.5. Monitorování a přezkoumávání rizik

Sledování, údržba a přezkoumávání rizik je poslední, avšak neméně důležitá součást systému řízení rizik. Stejně tak jako pro všechny ostatní fáze, by měla být prováděna revize současného stavu, a to alespoň jedenkrát za rok.

Aplikace usnadňuje správu databáze aktiv, hrozeb a zranitelností i výsledných hodnot rizik, umožňuje přepis hodnot rizik v závislosti na aktuálním stavu, neboť se mohou během doby jejího provozu měnit vnější i vnitřní podmínky a okolnosti, které rizika ovlivňují. [6]

4.6. Projekt vývoje webové aplikace

Tato činnost je pro oddělení nová, jedinečná, ohraničena mnoha faktory a z části neopakovatelná, proto by měla být řízena jako projekt. Oddělení nemá zavedeny oficiální postupy projektového řízení, proto budeme postupovat podle navrženého plánu v kapitole Plán postupu projektu. Zavádění projektového řízení do oddělení je nad rámec této práce. Zdrojové kódy budou umístěny v komprimovaném souboru jako příloha této práce.

4.6.1. Plán postupu projektu

Stanovení realistického cíle, zjištění potřebných informací a provedení důkladných analýz, vývoj, testování a provoz jsou postupné činnosti projektu. Evidenci informací o těchto činnostech nalézáme v identifikační listině projektu, která je vstupním dokumentem k řešení projektu a je důležitá i pro jeho úspěšné dokončení. [21] Našim cílem je vyvinout takovou aplikaci, která usnadní správu systému řízení bezpečnosti informací, a tím také napomůže zvýšit bezpečnost v oddělení.

Tabulka 9: identifikační neboli zadávací listina projektu vývoje aplikace (Vlastní zpracování dle: [21])

Název projektu	**Vývoj webové aplikace na analýzu rizik**
Identifikátor projektu	***ID01***
Záměr (může být více):	Zlepšení bezpečnosti informací v oddělení, Usnadnění provádění analýzy rizik a uchovávání výsledků.
Cíl (pouze jeden):	Navrhnout webovou aplikaci pro analyzování rizik, užitnou v kombinaci se systémem řízení bezpečnosti informací pro usnadnění správy a zvýšení bezpečnosti v organizaci, a popsat tento návrh v diplomové práci.
Zadavatel projektu (interní):	Vedoucí oddělení
Zainteresované strany (externí):	CERT/CSIRT bezpečnostní týmy Ostatní zaměstnanci KaM Zákazníci
Manažer projektu (odpovědný):	Vedoucí oddělení

Projektový tým (funkce + jméno):	Vývojář Tester
Výstupy projektu (více):	Webová aplikace na analýzu rizik integrovaná do informačního systému oddělení.
Plánované interní (přímé) náklady:	Uvedeny v tabulce nákladů jako mzdové náklady
Plánované externí náklady:	----------
Plánovaný termín zahájení:	23.09. 2019
Plánovaný termín ukončení:	01.05. 2020
Milníky projektu:	**do 31. 12. 2019** – vyhotovení pragmatické AR a sběr dat **do 29. 02. 2020** – konstrukce platformy pro vývoj **do 01.04. 2020** – vývoj **13. 04. – 27. 04. 2020** – testování a integrace **01. 05.** – plánované ukončení projektu
Umístění projektu:	projekt je tvořen a testován lokálně, integrace bude provedena po fázi testování

Schválení projektu	
Schváleno dne:	
Schválil:	***Podpis:***

Abychom správně odhadli časovou náročnost projektu, provedeme dekompozici celého projektu na jednotlivé činnosti pomocí metody Work Breakdown Structure (zkr. WBS). Postup jednotlivých činností na 3. úrovni a dále, je již vlastní provedení úkolu a spadá pod odpovědnost předem určených pracovníků. [21]

WBS	komplexní projekt	
1. úroveň	*2. úroveň*	*3. úroveň*
Vývoj, integrace a provoz weobvé aplikace na analýzu rizik	1. předprojektové analýzy	1.1. definování SMART cíle
		1.2. analýza vnějších faktorů
		1.3. analýza vnitřních faktorů
		1.4. analýza rizik projektu
		1.5. SWOT
	2. vývoj	2.1. sběr dat
		2.2. pragmatická analýza rizik
		2.3. příprava infrastruktury
		2.4. příprava prostředí
		2.5. vývoj
		2.6. testování
	3. zavádění	3.1. zavádění organizační změny
		3.2. zavádění HW a SW
		3.3. zavádění dokumentace
		3.4. zavádění školení personálu
	4. provoz	4.1. spuštění do provozu
		4.2. monitorování
		4.3. přezkoumávání

Obrázek 21: WBS komplexního projektu (Vlastní zpracování dle: [21])

V následujících kapitolách by měly být stanoveny technologie pro realizaci a také určíme základní prvky vývoje jako rozvržení souborové struktury, provázanost jednotlivých částí a grafické prvky. Dalším krokem je testování validity webových stránek, k čemuž můžeme využít například online validátor společnosti W3C. Také klademe důraz na test rozložení a fungování napříč různými webovými prohlížeči, neboť různý software může reagovat na kód různě. Vzhledem k způsobům a četnosti použití aplikace pravděpodobně nebude nutné vytvářet speciální mobilní verzi webové aplikace, určenou pro zařízení typu smartphone, tablet apod. [11]

4.6.2. Pragmatická analýza informačních rizik

Pro vývoj aplikace bylo zapotřebí zpracování pragmatické analýzy informačních rizik, využijeme tak zjednodušeného a neformálního postupu abychom dokázali nastínit

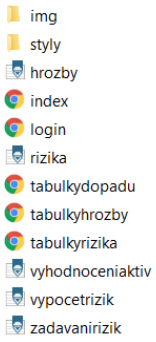
činnosti analyzování i s výsledky, a snadněji je transformovali do prostředí webu a databáze, neboť pro vývoj nevyužíváme žádnou šablonu. [1]

4.6.3. Příprava prostředí pro aplikaci

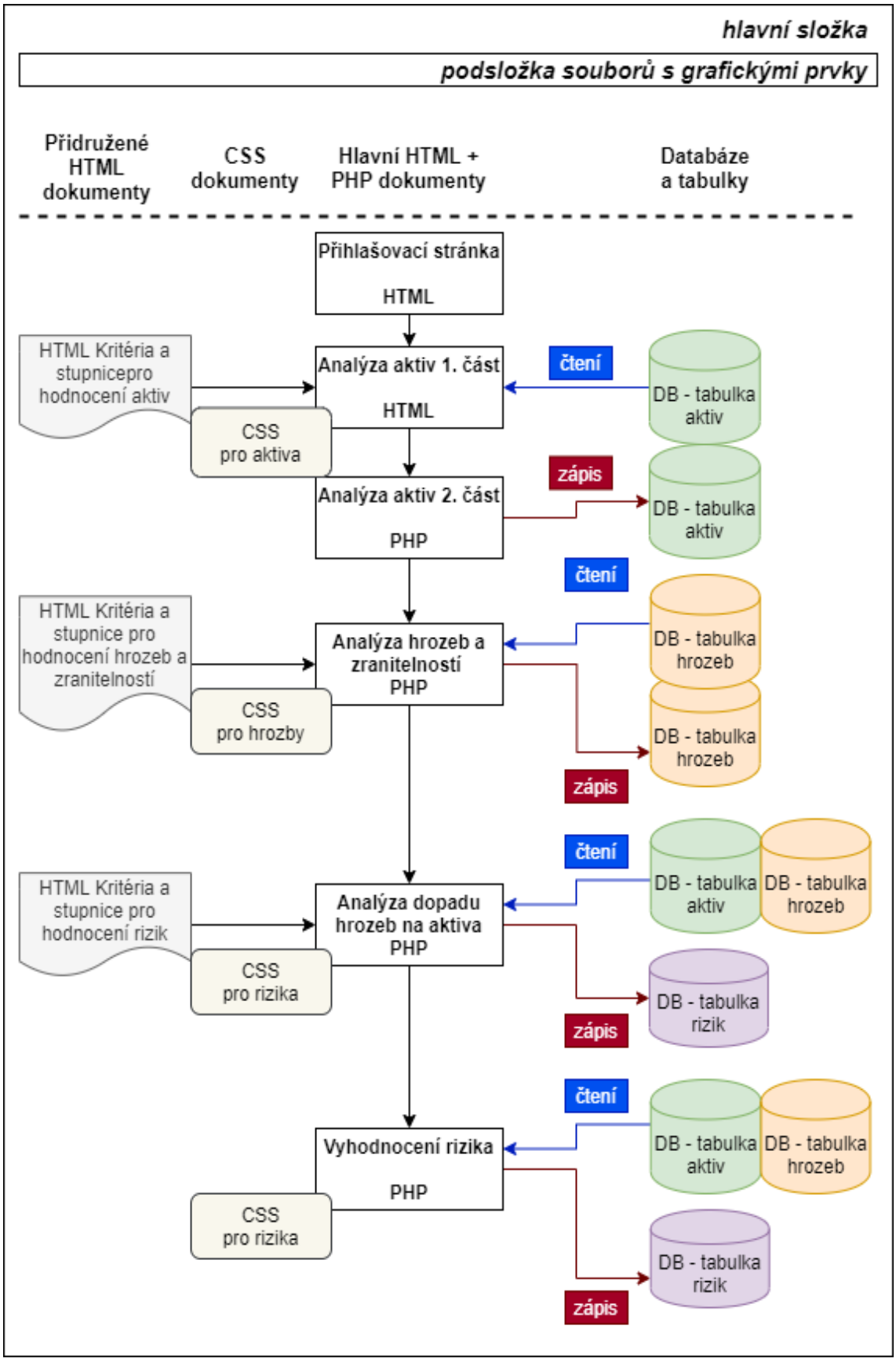
Vzhledem k nepřetržitému provozu počítačové sítě i informačního systému jsme zvolili pro vývoj oddělené HW prostředky, na kterých bude zároveň testován provoz aplikace. Pro provoz aplikace není vyžadován vysoký výpočetní výkon ani kapacitně náročná úložiště. Pro vývoj a testování bylo nutné zprovoznit webový server. S ohledem na již používané technologie, dostupnost a náklady byl vybrán softwarový webový server Apache, jehož instance byla lokálně instalována do operačního systému, a veškeré ladění webových stránek probíhalo vůči tomuto serveru. Dále byla využita relační databáze MariaDB, která je vydávána s licencí GNU/GPL, ta je pro software s otevřeným kódem typická, a je kompatibilní s prostředky, které využívá oddělení. Pro zjednodušení správy tabulek i databáze byl využit softwarový nástroj phpMyAdmin v jehož prostředí lze pracovat s příkazy v jazyce SQL, ale i využít uživatelského rozhraní. [11] [17]

4.6.4. Rozvržení souborové struktury

Pevný základ každé webové aplikace je vhodné rozložení souborové struktury, měla by být udržována jednoduchá, aby byla zajištěna přehlednost. Dále jednotlivé dokumenty by měly být věcně pojmenovány, nejlépe bez využití diakritiky, neboť při přenášení do jiných adresářů, v jiných operačních systémech, může s použitím diakritiky vyvstat problém a také smysluplně uspořádaná, aby bylo možné jednotlivé dokumenty snadno upravovat. [11] Z tohoto důvodu je souborová struktura rozvržena do několika málo souborů, jak můžeme vidět na obrázku níže.



Obrázek 22: dokumenty a podsložky v kořenové složce (Vlastní zpracování)



Obrázek 23: souborová struktura webové aplikace (Vlastní zpracování)

4.6.5. Použité prostředky

Pro vizuální stránku webové aplikace bylo použito tzv. Cascading Style Sheets (zkr. CSS). Tento programovací jazyk popisuje způsob zobrazení webových stránek kódovaných v HTML, XML nebo XHTML. Byl vytvořen za účelem oddělení vzhledu dokumentu od jeho obsahu. Jsou-li jednotlivé části aplikace spojeny v jednom kódu, ztrácí se přehlednost a lze se v něm jen těžko vyznat. Samotná grafika je vytvořena v programu Photoshop, který byl vhodným nástrojem pro všechny použité prvky. Vždy nejprve uvádíme název prvku a poté do složených závorek vepisujeme nastavovaný styl prvku. [11][12]

```
body {
    text-align: center;
    margin: 0px;
    border: 0px solid silver;
    padding: 0px;
    font-family: Arial, Helvetica, sans-serif;
}
.hlavicka {
   text-align: left;
   margin-left: 0px;
   padding: 0px;
   border: none;
}
a.logocvis{
   margin-left: 0px;
   padding: 0px;
}
div {
   border: 5px solid silver;
}
table {
    border-spacing: 0px;
    border: 1px solid black;
    width: 1000px;
    margin-top: 10px;
}
label{
    color:grey;
}

```

Obrázek 24: ukázka CSS kódu v editoru PSPad (Vlastní zpracování)

4.6.6. Použité protokoly

Internetový protokol Hyper Text Transfer Protocol (nebo jeho zabezpečená verze HTTPS), který slouží pro výměnu hypertextových dokumentů kódovaných značkovacím jazykem HTML a případně v jiných jazycích, využívá jednoznačného umístění zdroje v internetu, které je specifikované v tzv. Uniform Resource Locator (URL). Protokol komunikuje způsobem dotaz-odpověď, tedy uživatel odešle dotaz ve formě textu přes klienta (obvykle webový prohlížeč) a server nazpět odesílá textovou odpověď s popisem výsledku dotazu a samostatnými daty požadovaného dokumentu. [11]

Soustava propojených hypertextových dokumentů, jinak také aplikace internetového protokolu HTTP, tvoří dohromady World Wide Web (www). [11]

```
<!DOCTYPE HTML>
<html lang="en">
 <head>
    <meta charset="UTF-8">
    <title>Přihlášení do aplikace</title>
    <link rel="icon" type="image/png" sizes="32x32" href="img/favicon-32x32.png">
    <link rel="stylesheet" type="text/css" href="styly.css">
 </head>
 <body>
  <div class="hlavicka">
   <a href="http://www.vutbr.cz" class="logocvis"><img src="img/CVIS.png" alt="na VUT" /></a>
  </div>
    <img src="./img/knlog.png" alt="logo" />
     <h1>ANALÝZA  RIZIK</h1>
       <form name="login" >
        <div class="login">
         <label for="login">PŘIHLAŠOVACÍ JMÉNO:</label>
          <input type="text" id="login" name="userid" size="50" style="border: 3px solid grey" />
         <label for="pas">HESLO:</label>  <br />
          <input type="password" id="pas" name="pswrd" size="50" style="border: 3px solid grey"  />
          <input type="button" onclick="kontrola(this.form)" value="PŘIHLÁSIT" style="border: 4px solid grey" />
        </div>
       </form>
```

Obrázek 25: ukázka HTML kódu přihlašovací stránky v PSPad (Vlastní zpracování)

4.6.7. Použité programovací jazyky

Základním programovacím jazykem je značkovací jazyk Hyper Text Markup Language (HTML). Jsou pro něj typické tzv. tagy neboli značky a jejich jednotlivé atributy. Mezi tyto značky se uzavírá text dokumentu, a tím je určen význam tohoto textu. Existují startovací a ukončovací značky, a jejich názvy se uzavírají do úhlových závorek (< a >). Jako element pak označujeme celek tvořený oběma druhy značek a požadovaným obsahem. [11]

Dalším použitým jazykem je JavaScript, tento objektově orientovaný skriptovací jazyk lze použít na různých platformách, a jsou jím nejčastěji ovládány různé interaktivní prvky. Často se setkáváme s tím, že je JavaScript kód vkládán přímo do HTML kódu.

Hlavním skriptovacím programovacím jazykem v této práci je Hypertext Preprocessor (zkráceně PHP). Je velmi hojně využíván při programování webových aplikací, zejména kvůli jednoduchosti, velké zásobě interních funkcí a kombinaci dobrých vlastností více programovacích jazyků. [11]

```
    //výpočet rizika
    $p= 0;
    $q= 1;
    $r= 11;

    for ($pom=1;$pom<=$pocetn;$pom++){

     $dopad = $_POST["$radek&$pom"];        //prim.php input name je 11&1, 11&2.....
     $dopadnum = (int)$dopad;

     $hp = $_POST["$pom&hod"];          //prim.php input name je 1&hod, 2&hod.....
     $hpnum = (int)$hp;
     $p=$p+1;

     $vysledek3 = $dopadnum*$hpnum;

    if ($vysledek3>=10) {
     echo '<td indexX='.$radek.' indexY='.$pom.' style="background-color:#db2c2c">'.$vysledek3."</td>";
    } elseif ($vysledek3>=5 && $vysledek3<10)
    {
     echo '<td indexX='.$radek.' indexY='.$pom.' style="background-color:#ff7f16">'.$vysledek3."</td>";
    } else
    {
     echo '<td indexX='.$radek.' indexY='.$pom.' style="background-color:#03b67b">'.$vysledek3."</td>";
    }
}
    $r=$r+1;
   $radek=$radek+1;
 echo"</tr>";
}
}
```

Obrázek 26: část funkce pro výpočet rizika v editoru PSPad (Vlastní zpracování)

4.6.8. Grafické uživatelské rozhraní

Aby byla aplikace dobře využitelná je vhodné již při vývoji myslet také na její praktickou stránku. Prvky jako hlavička, tlačítka, popisy a tabulky jsou logicky uspořádané tak, aby jasně definovaly svůj účel a byly dobře viditelné a čitelné. Rozložení těchto prvků se během práce s aplikací mění pouze minimálně a spíše se uzpůsobuje obsahu, uživatel tak dokáže intuitivně vyhledat daný prvek, obvykle je totiž umístěn na stejném místě v rozložení webu, jako na předchozí stránce. Aplikace však není tvořena kvůli svému designu, ale především aby urychlila pracovní procesy v oddělení, je tedy velmi jednoduše vizuálně uspořádaná. Přestože se menu všech webových stránek v informačním systému oddělení vyskytuje svisle na levé straně obrazovky, v tomto případě je umístěno vodorovně v horní části stránky. Pod menu tak vznikne prostor, který dobře využijeme pro rozsáhlé tabulky analýz. Použité barvy jsou zvolené podle

kombinace barev oficiálního loga organizačně nadřazené jednotky (červená a šedá) a barev, které ve svém IS využívá oddělení (šedá).

Obrázek 27: rozložení hlavičky a tlačítek u aktiv (Vlastní zpracování)

Obrázek 28: obdobné rozložení hlavičky a tlačítek u hrozeb (Vlastní zpracování)

Barevně oddělené a zvýrazněné jsou vždy tabulky hodnocení (červená tlačítka v pravé části menu), po kliknutí se otevřou na nové záložce, obsluha aplikace tak může snadněji vypisovat potřebné hodnoty, aniž by se v prohlížeči pokaždé vracela na předešlou webovou stránku.

4.6.9. Databáze s daty

Použitá relační databáze je tvořena ze tří tabulek s relačními vazbami, která slouží jako zdroj aktuálních i historických dat. Přestože jsou pro historická data vhodnější datové sklady, vzhledem k malému množství dat a jejich časté aktualizaci, splní relační databáze svůj účel dostatečně. Sloupce jednotlivých tabulek byly určovány postupně podle postupu činností v pragmatické analýze rizik, tak aby při vyhodnocování analýzy nechyběla žádná data.

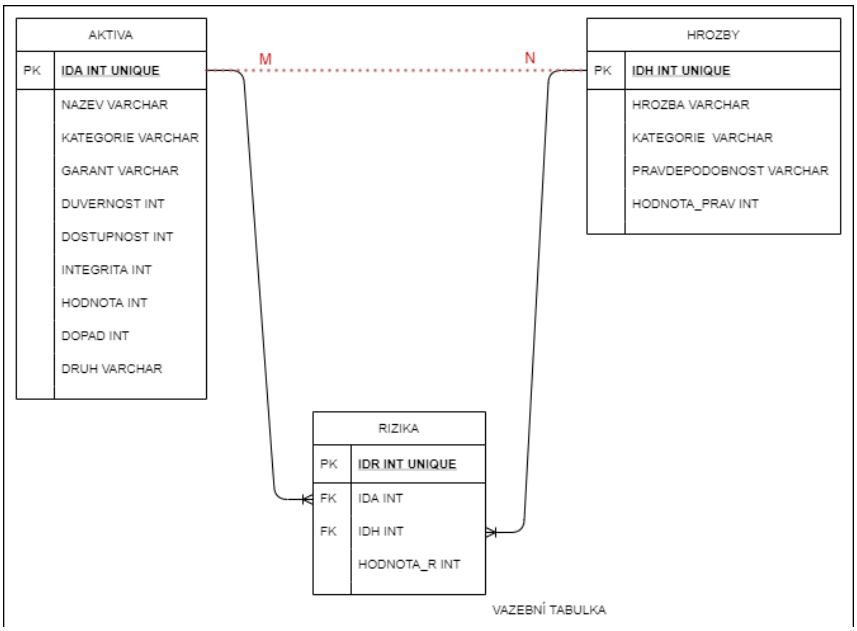
Datové typy jednotlivých sloupců jsou definovány na základě ukládaného obsahu, číselné hodnoty jsou ve všech případech datového typu Integer (INT), který pracuje s celými čísly v dostatečném rozsahu. U některých atributů je délka ukládaných znaků omezena, zejména u sloupců s hodnocením podle zadaných stupnic, kdy nevyužijeme při analýze

jiné hodnoty, než jsou stanoveny v těchto stupnicích. Textová pole jsou datového typu Varchar(M), kde M představuje maximální počet znaků z rozsahu (0 až 65 532 znaků) a tyto jejich délky jsou opět přizpůsobeny ukládanému obsahu polí. Sloupce označené jako primární klíče mají oproti ostatním navíc vlastnost AUTO_INCREMENT, která dokáže generovat postupné číselné hodnoty datového typu INT, tuto vlastnost jsme využili pro generování identifikátorů, které vyžadují také jedinečnost záznamu. [17]

#	Name	Type	Collation
1	**nazev**	varchar(50)	utf8_czech_ci
2	**kategorie**	varchar(50)	utf8_czech_ci
3	**garant**	varchar(50)	utf8_czech_ci
4	**duvernost**	int(2)	
5	**dostupnost**	int(2)	
6	**integrita**	int(2)	
7	**hodnota**	int(2)	
8	**dopad**	int(2)	
9	**druh**	varchar(50)	utf8mb4_czech_ci
10	**ida** 🔑	int(11)	

Obrázek 29: atributy tabulky aktiv v programu phpMyAdmin (Vlastní zpracování)

Relační diagram zobrazuje databázové tabulky a jejich atributy a relační vazby mezi těmito tabulkami. Relační vazba mezi tabulkami aktiv a hrozeb M:N, byla dekomponována pomocí vazební tabulky na dvě vazby 1:N, jak můžeme vidět na obrázku níže.



Obrázek 30: E-R diagram (Vlastní zpracování)

Práce s databází probíhá během celého procesu analyzování, čtení (SELECT) a zápis (INSERT) doplňujeme také dalším příkazem UPDATE, kdy je možné již uložená data aktualizovat na nové hodnoty, v případě, že bude vyžadován přepis hodnot. Následující příkaz obsahuje kromě `SELECT` také `COUNT(*)`, takto lze spočítat počet prvků uložených v databázi podle určité podmínky. Zde jako výsledek získáme počet hrozeb, které mají identifikátor větší jak 1.

```
$queryjedna = "SELECT COUNT(*) as pocet FROM `hrozby` WHERE `id` > 1" ;
$pocet = (pocethrozeb($queryjedna));
```

Obrázek 31: příklady příkazů SELECT pro práci s databází (Vlastní zpracování)

V jiném případě využijeme `UPDATE`, abychom přepsali hodnotu rizika specifikovaného podle identifikátoru rizika `IDR`, v tabulce `RIZIKA` na novou hodnotu proměnné `$vysledek`.

```
$sql = "Update `rizika` SET `hodnotar`= $vysledek WHERE IDR=$i";
```

Obrázek 32: příklad příkazu UPDATE pro práci s databází (Vlastní zpracování)

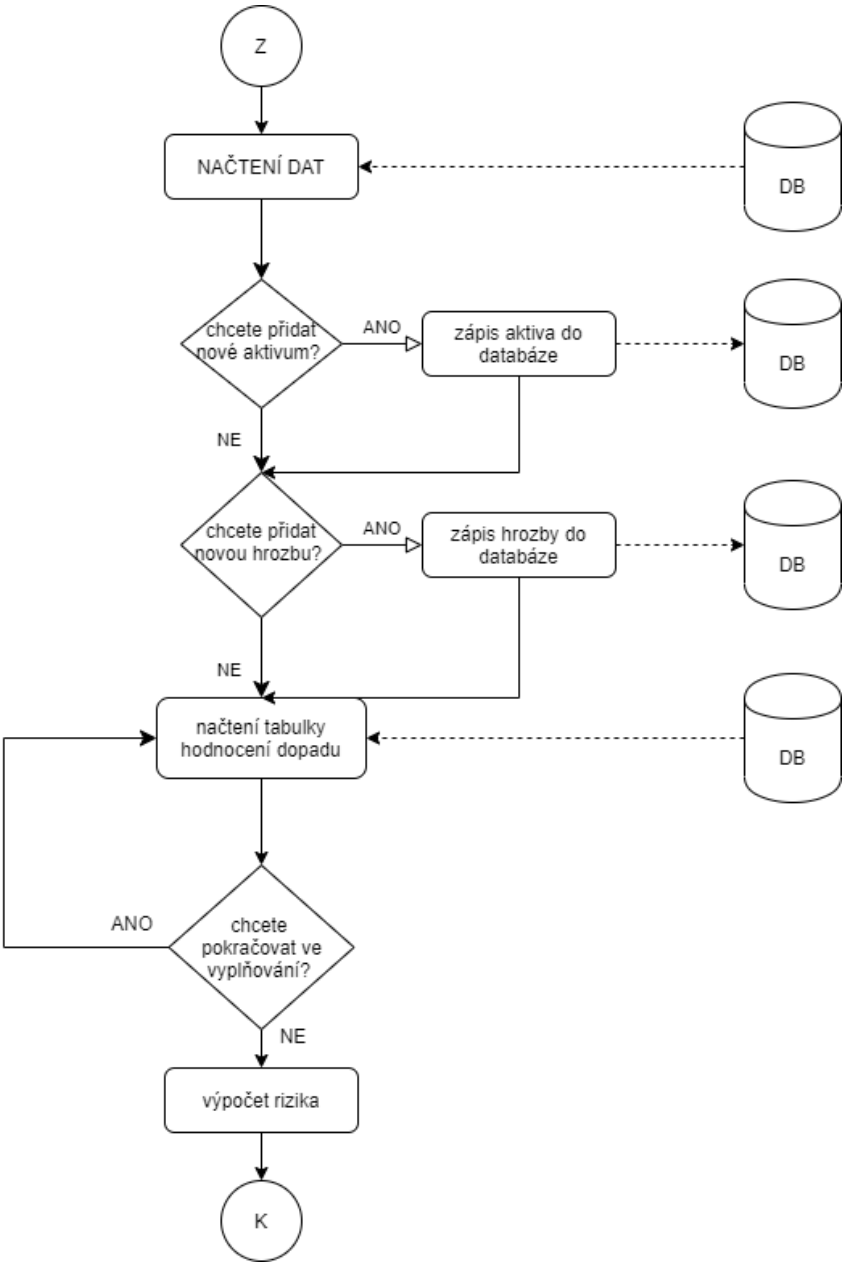
4.6.10. Znaková sada a kódování znaků

Další důležitou součástí všech použitých softwarových nástrojů je znaková sada a kódování znaků. Předdefinované hodnoty jednotlivých softwarových programů musely být upraveny, aby při práci s daty nedocházelo ke ztrátě znaků s diakritikou. Úprava proběhla na databázovém serveru, databázi i jednotlivých sloupcích v tabulkách a stejně tak vyžadovaly úpravu kódování všechny dokumenty v souborové struktuře webové aplikace. Znaková sada byla použita UTF-8 a kódování znaků bylo upravováno dle možností softwarového vybavení, tak aby byla udržena kompatibilita všech systémů. [17]

4.6.11. Integrace do prostředí

Integrace aplikace a s ní související nový pracovní proces se projeví v celém oddělení, a proto rozhodnutí o zavedení závisí na vedení oddělení. S integrací je spojen také vznik nové dokumentace a interních pravidel, které bude opět nutné zanést do IS. Nejvíce ale integrace ovlivní pracovníky. V určité fázi bude nutné zaškolit pro práci s aplikací nejprve pracovníky bezpečnosti informací a poté také všechny ostatní pracovníky.

Školení pro pracovníky informační bezpečnosti, pod které spadá také obsluha aplikace, by mělo být ve větším rozsahu, vedeno pracovníky, kteří se na vývoji a testování podíleli a může být zahrnuto do komplexnějšího systému školení informační bezpečnosti obecně. Pro ostatní pracovníky pak postačí stručné školení s informacemi o zavedení a provozu aplikace, co aplikace přinese a jak se mají zaměstnanci podílet na monitorování a přezkoumávání aplikace, případně jak mají poskytovat zpětnou vazbu. Nový pracovní proces by se měl také propsat do všech stávajících dokumentů a souborů, které pracovní procesy evidují.



Obrázek 33: diagram procesu analýzy rizik v aplikaci (Vlastní zpracování)

4.6.12. Přístup do aplikace

Přístup do aplikace bude možný zásadně pro pověřené pracovníky bezpečnosti. Samotný informační systém je ve své obsáhlejší administrátorské verzi zabezpečen kombinací přístupových údajů (přihlašovací jméno a heslo) a osobního certifikátu. Jedná se tedy o dvou-faktorou autentizaci do systému. Pro přístup do webové aplikace je vytvořena oddělená přihlašovací webová stránka, která obsahuje formulář s polem pro vyplnění přihlašovacího jména a hesla. Data, která aplikace obsahuje přísluší do administrátorského prostředí a měla by být důkladně zabezpečena.

4.6.13. Práce s aplikací

Pověřená osoba neboli obsluha aplikace, manipuluje s daty pouze v rozsahu stanoveném možnostmi aplikace. Zároveň je tato práce v provozu řízena dokumentovanou směrnicí Metodika analýzy rizik, která je uvedena v příloze. Větší změny v aplikaci je výrazně doporučeno konzultovat vedením. Aplikace je navržena tak, aby usnadnila a urychlila analyzování rizik a prvky aplikace jsou rozmístěny tak, aby naváděly uživatele k dalším správným krokům a zbytečně ho nezatěžovaly dlouhými texty s návody k obsluze. Následující obrázky zobrazují jednotlivé kroky analýzy v aplikaci.

Obrázek 34: přihlašovací stránka (Vlastní zpracování)

Prvním krokem je, jak již bylo zmíněno, přihlášení do aplikace. Aplikace je naprogramovaná pro přihlášení pomocí přihlašovacího jména a hesla.

Název aktiva	Kategorie aktiva	Zdroj/Garant	Důvěrnost	Dostupnost	Integrita	HODNOTA	Dopad	DRUH
zadejte název aktiva	vyberte kategorii	zadejte zdroj	zadej hodnotu důvěrnosti	zadej hodnotu dostupnosti	zadej název integrity		zadejte hodnotu dopadu	
Aktivní zařízení pro zprac.	HW	Vedoucí	5	5	5		6	primární
Přenosná zařízení	HW	Vedoucí/Správce	4	5	4		4	podpůrné
Pevná zařízení	HW	Vedoucí/Správce	3	3	3		4	podpůrné
Procesní periferie	HW	Vedoucí	3	4	4		4	podpůrné
Pasivní nosiče dat	HW	Vedoucí	4	4	5		4	podpůrné
Elektronické nosiče dat	HW	Vedoucí	2	2	2		2	podpůrné
Ostatní nosiče (pap. dokur	HW	Vedoucí	2	2	2		2	podpůrné
Zákaznická/uživatelská zai	HW	Zákazník	3	3	3		4	podpůrné
Operační systémy	SW	Vedoucí	5	6	5		6	primární
Software pro správu	SW	Vedoucí	4	5	5		5	primární

Obrázek 35: analýza aktiv (Vlastní zpracování)

Obrázek 35. zobrazuje katalog aktiv a jejich analýzu. Zde se poprvé objevuje možnost zobrazit hodnotící tabulky pro hodnocení dostupnosti, důvěrnosti a integrity, jak tyto tabulky vypadají vidíme na dalším obrázku.

Obrázek 36: hodnotící tabulky pro aktiva (Vlastní zpracování)

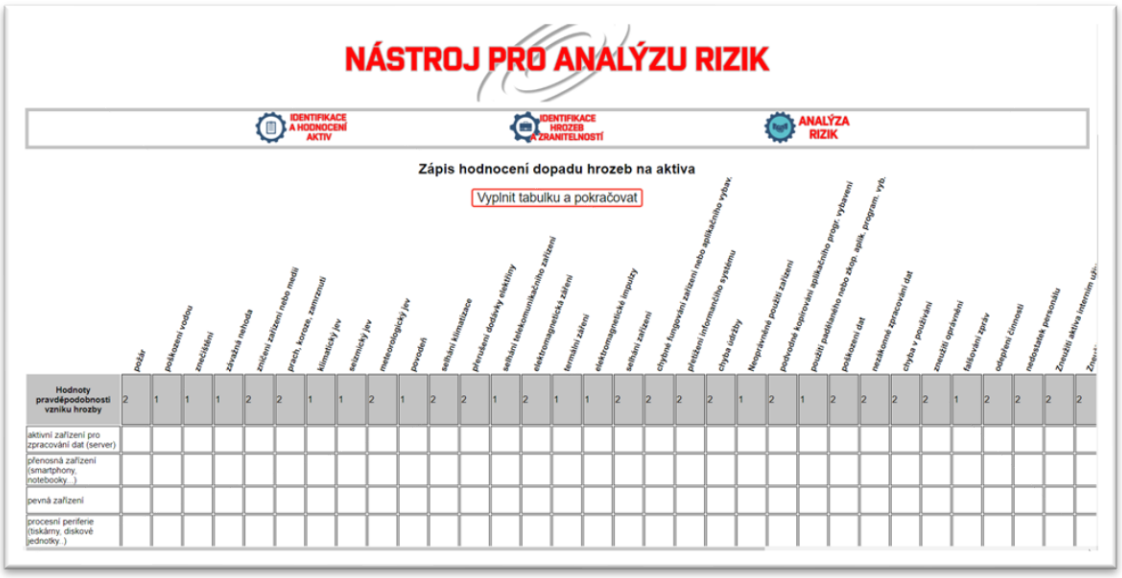
V případě, že vložíme nové aktivum, přejdeme ještě před vstupem do katalogu hrozeb na stránku shrnutí analýzy aktiv, na této stránce můžeme zkontrolovat nové záznamy a jejich správnost. Po analýze aktiv přecházíme na analýzu hrozeb, i zde nacházíme dvě možnosti, vložit novou hrozbu či přejít na další krok, kterým je hodnocení rizik. I u hrozeb nalezneme hodnotící tabulky, tyto dokumenty jsou vždy s příponou HTML.

Hrozba	Kategorie	Pravděpodobnost	Hodnota pravděpodobnosti.
zadejte název hrozby	zadejte kategorii	zadejte pravděpodobnost	
požár	environmentální a fyzické	střední	2
poškození vodou	environmentální a fyzické	malá	1
znečištění	environmentální a fyzické	malá	1
závažná nehoda	environmentální a fyzické	malá	1
zničení zařízení nebo médií	environmentální a fyzické	střední	2
prach, koroze, zamrznutí	environmentální a fyzické	střední	2
klimatický jev	environmentální a fyzické	malá	1
seizmický jev	environmentální a fyzické	malá	1
meteorologický jev	environmentální a fyzické	střední	2
povodeň	environmentální a fyzické	malá	1
selhání klimatizace	technická selhání	střední	2
přerušení dodávky elektřiny	technická selhání	střední	2
selhání telekomunikačního zařízení	technická selhání	malá	1
elektromagnetická záření	pochury způsobené zářením	střední	2
termální záření	pochury způsobené zářením	malá	1
elektromagnetické impulzy	pochury způsobené zářením	malá	1
selhání zařízení	technická selhání	střední	2
chybné fungování zařízení nebo aplikačního vybav.	technická selhání	střední	2
[illegible]	[illegible]	[illegible]	[illegible]

Obrázek 37: analýza hrozeb a zranitelností (Vlastní zpracování)

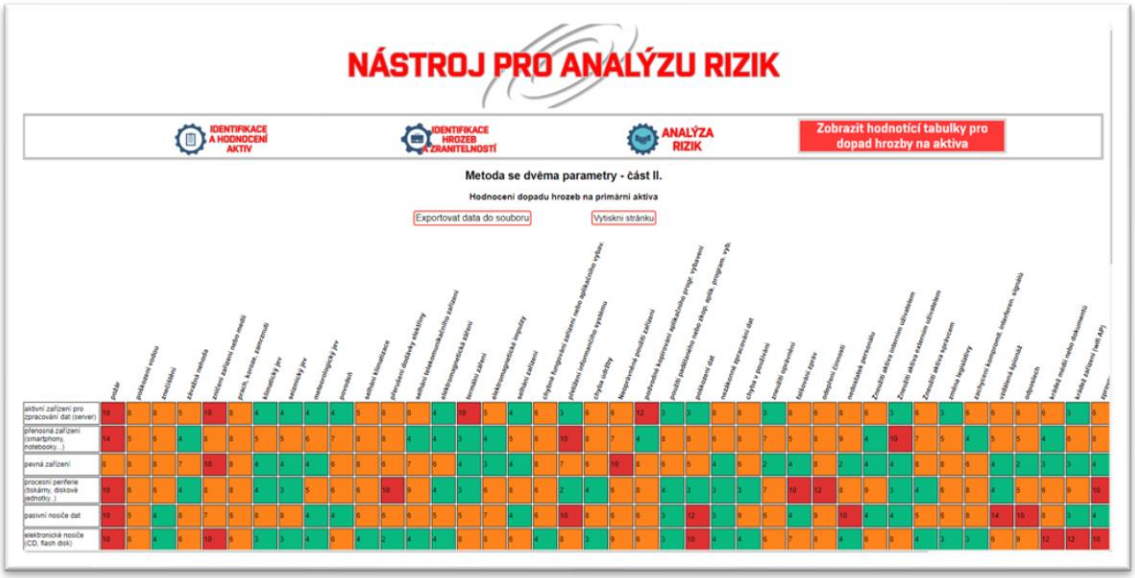
Úroveň (pravděpodobnost)	Popis (hodnota)
malá	1
střední	2
velká	3

Obrázek 38: hodnotící tabulky pro hrozby (Vlastní zpracování)



Obrázek 39: velká tabulka pro hodnocení dopadu hrozby na aktiva (Vlastní zpracování)

Obrázek 40: hodnotící tabulky pro rizika (Vlastní zpracování)



Obrázek 41: velká tabulka s riziky po doplnění (Vlastní zpracování)

Pro vyhodnocení rizika nejprve potřebujeme určit dopad hrozby na specifické aktivum, k tomu slouží tabulka na obrázku 39, která je tvořena mnoha políčky k vyplnění obsluhou aplikace.

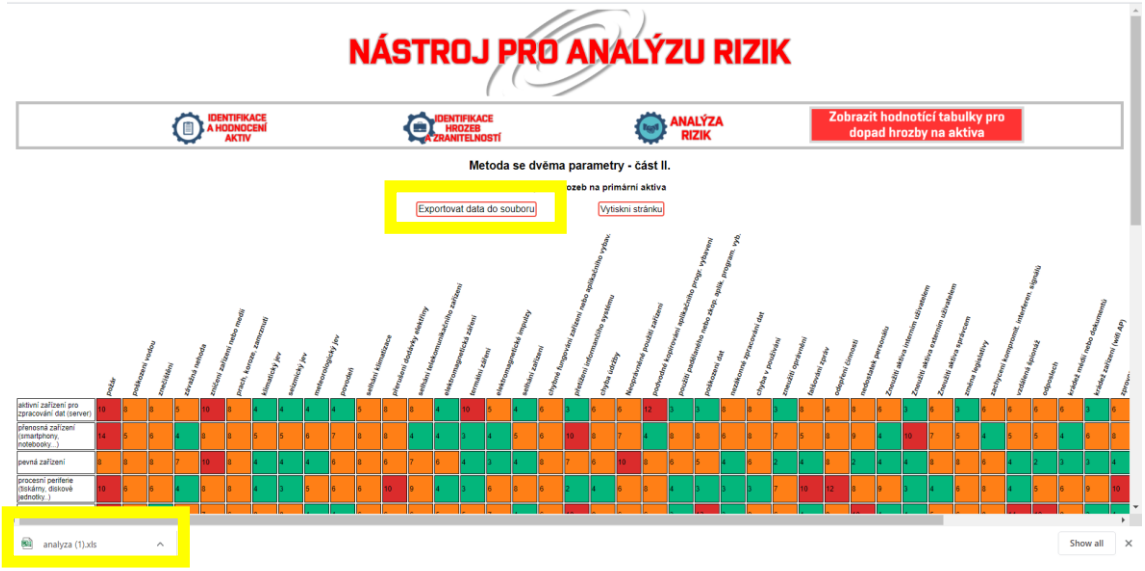
Důležité je vědět, že obsluha nemusí vyplňovat pokaždé všechna pole znovu, ale stačí vyplnit pouze všechna pole spojená s nově přidanými aktivy či hrozbami a případně upravit hodnoty u původních aktiv a hrozeb v případě, že se během cyklu pro přezkoumávání systému řízení bezpečnosti informací, a tedy i analyzování rizik, změnily,

zbylé hodnoty se doplní z databáze automaticky (objeví se historická data z předešlé analýzy rizik).

Jednotlivé hodnoty jsou podbarveny podle významnosti rizika. Červená značí nejvýznamnější riziko, a tedy riziko s nejvyšší prioritou. Oranžová značí riziko přijatelné za podmínky, že jsou náklady na řízení rizika neúměrně vysoké oproti způsobeným škodám. Zelená představuje riziko nevýznamné, na které není nutné aplikovat opatření.

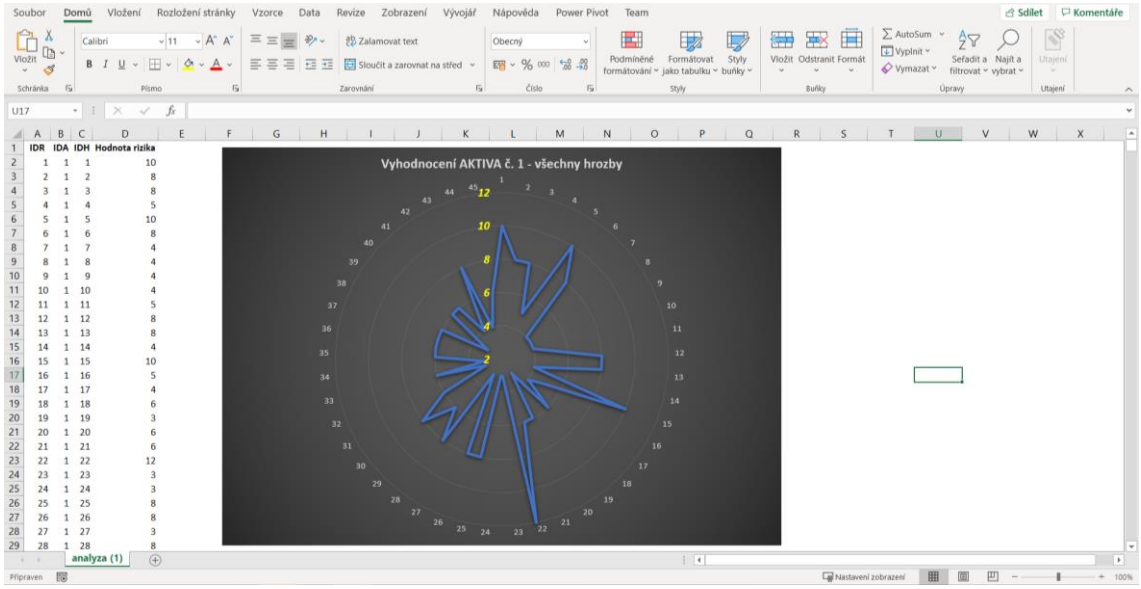
4.6.14. Export dat

Získaná data z analýzy rizik je možné exportovat jako tabulku do souboru s příponou .xls, tento typ souboru byl vybrán proto, aby bylo možné s daty dále pracovat (zejména vytvářet grafy). Tento soubor obsahuje tři identifikátory a výslednou hodnotu rizika ve čtyřech sloupcích. Bez aplikace samotné, nelze přiřadit hodnoty k jednotlivým aktivům a hrozbám a data jsou tak částečně zabezpečena před zneužitím v případě, že budou uchovávána nezašifrována, v otevřené formě.



Obrázek 42: export dat do souboru s příponou .xls (Vlastní zpracování)

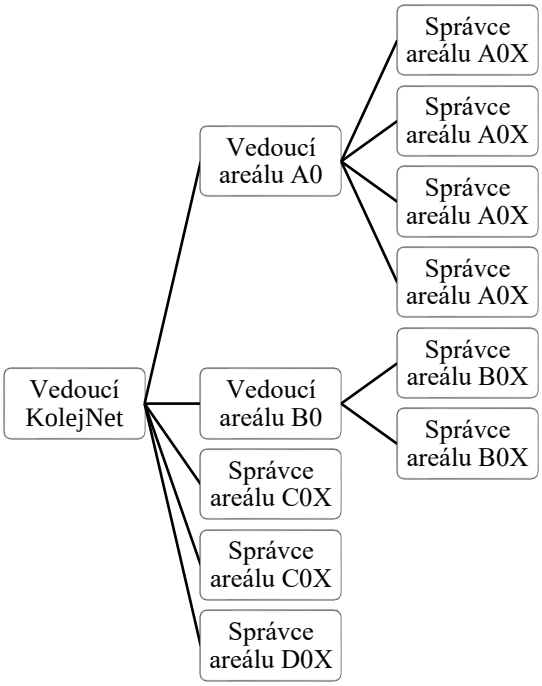
Na předchozím obrázku můžeme vidět stažený soubor s daty, se kterými lze nadále v excelu pracovat. I přesto, že jsou výsledky graficky oddělené i v aplikaci, pro lepší přehlednost je možné z dat generovat různé druhy grafů.



Graf 5: pavučinový graf zobrazující extrémy, vytvořený na exportovaných datech (Vlastní zpracování)

4.6.15. Obsluha aplikace

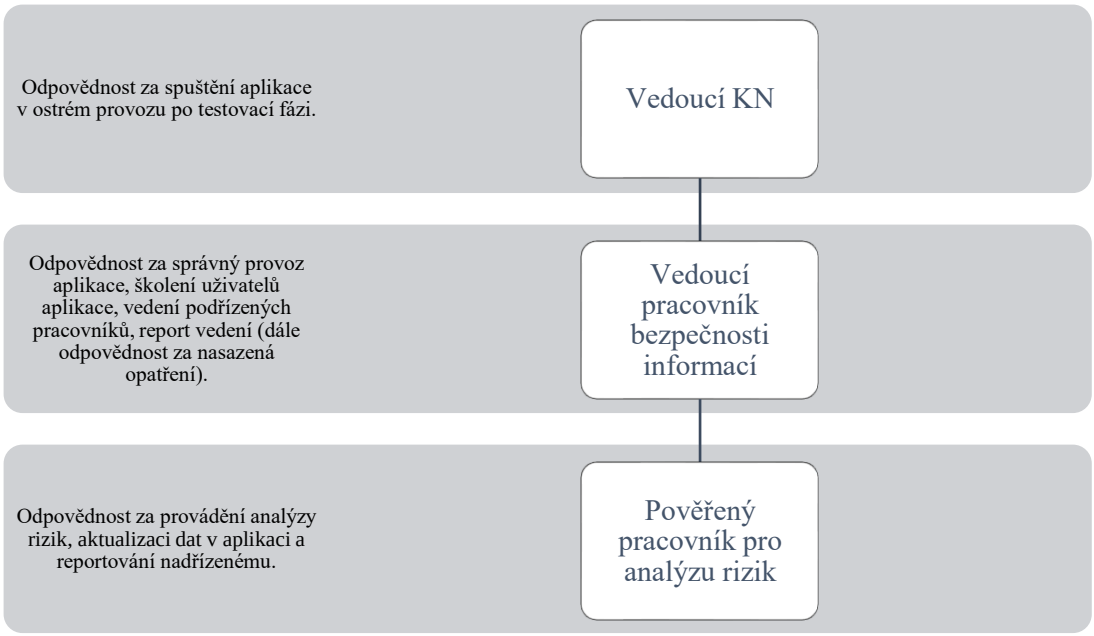
Organizační struktura pro analyzování rizik v oddělení je stanovena na základě organizace pracovních pozic, kterou zobrazuje následující diagram.



Obrázek 43: organizace všech pracovních pozic (Vlastní zpracování)

Na základě organizační struktury pracovních pozic jsme stanovili a upřesnili pozice pro práci s aplikací při analyzování rizik. Vedoucí pozice a pozice pověřeného pracovníka

pro provádění analýzy rizik by neměla být obsazena tentýž pracovníkem, v opačném případě by byl reportovací systém bezvýznamný.



Obrázek 44: organizace pracovníků v souvislosti s analýzou rizik (Vlastní zpracování)

4.7. Testování

Nedílnou součástí správně naprogramované webové aplikace je její testování. Nejedná se pouze o testování funkčnosti a správnosti získaných dat, ale také o validaci syntaxe, která vlastně znamená opravování chyb ve zdrojovém kódu webové stránky. Validování je důležité zejména z důvodu přehlednosti, zobrazování i rychlosti načítání. V případě, že je web validní, měl by se v různých prohlížečích zobrazovat stejně, pokud tomu tak není, je pravděpodobně chyba na straně prohlížeče. [11]

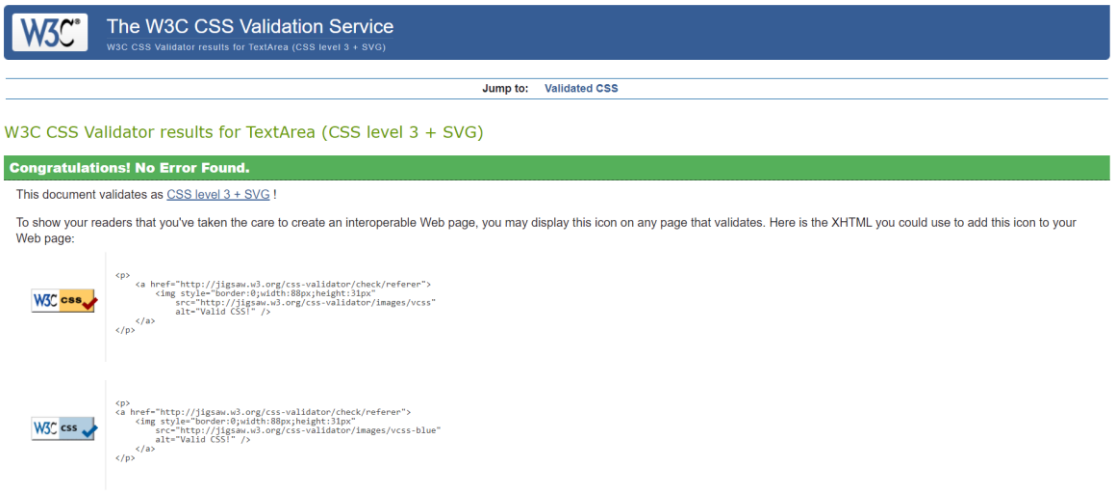
4.7.1. Testování funkčnosti a výpočtů

Tato část testování probíhala na datech pragmatické analýzy rizik. V případě, že počítaná pole generovala stejné výsledky jako byly zjištěny v pragmatické analýze rizik, vyhodnotil se algoritmus výpočtu jako správný.

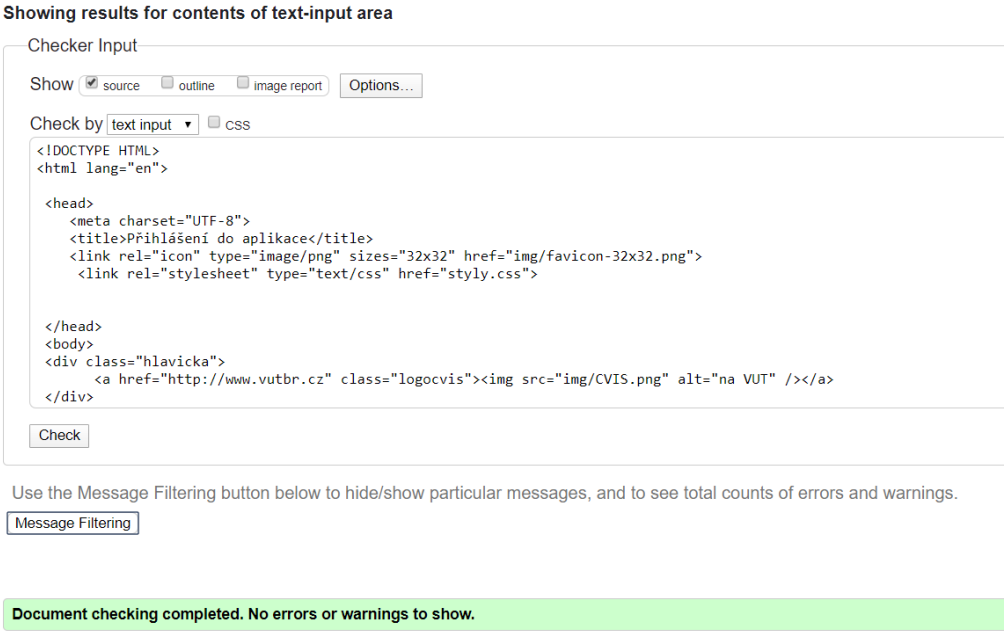
Ověřována byla také funkčnost komunikace s databází, tedy zápis a čtení dat. Používané příkazy SQL a jejich výsledky byly nejprve ověřovány v softwaru phpMyAdmin, pokud to charakter příkazu dovoloval, a až poté umístěny do dokumentu.

4.7.2. Testování validace

Validnost dokumentu se testovala na webových stránkách mezinárodní konsorcia W3C rozvíjející standardy a směrnice pro World Wide Web. Kontrola správnosti zápisu byla prováděna načtením celého individuálního souboru a ověřením. Validátor dokáže ověřovat různé typy webových stránek a vypisuje závažné chyby i varování v syntaxi jednotlivě, což podstatně usnadňuje opravu chyb. Na následujících obrázcích vidíme příklad výsledku validace přihlašovací stránky webové aplikace a validaci přidruženého CSS dokumentu. [19]



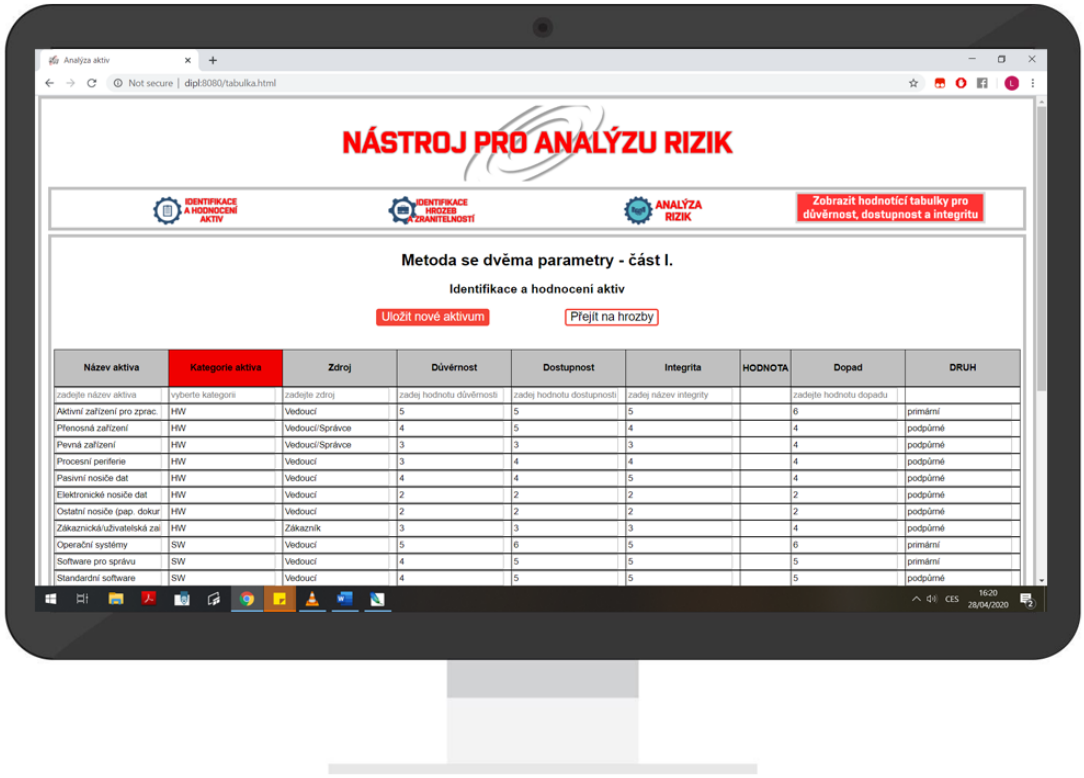
Obrázek 45: testování validace CSS dokumentu (Zdroj: [19])



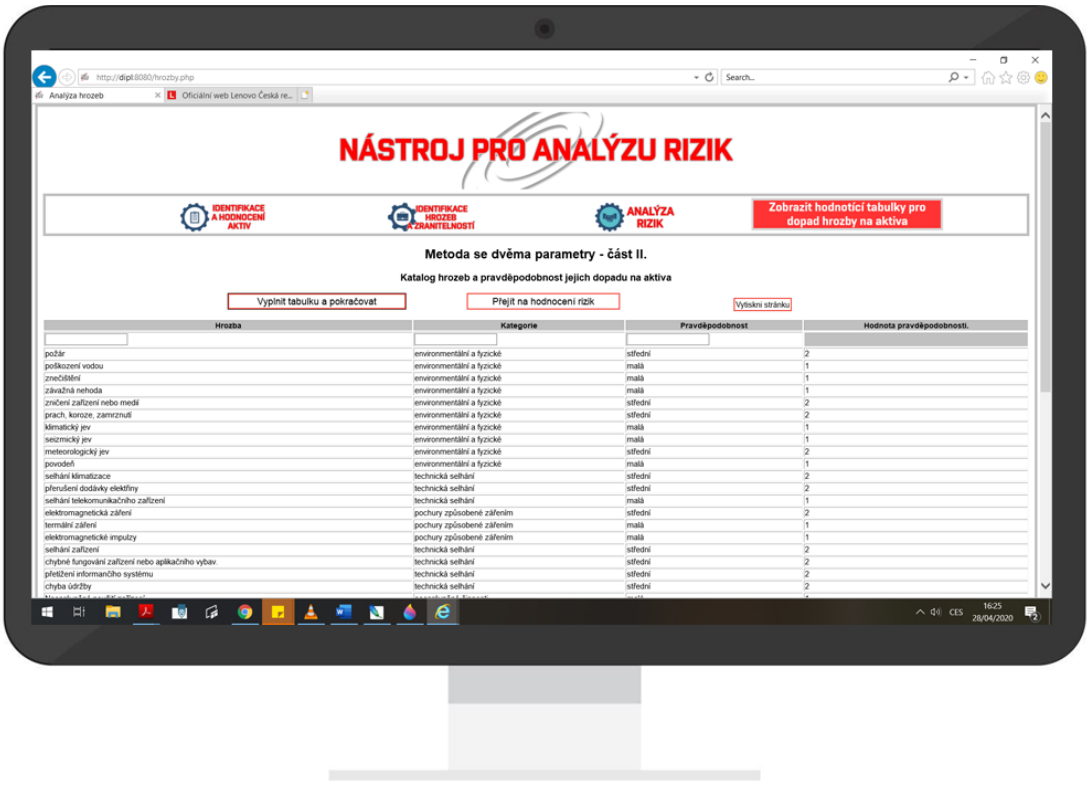
Obrázek 46: proces online validace webových stránek (Zdroj: [19])

4.7.3. Testování zobrazení

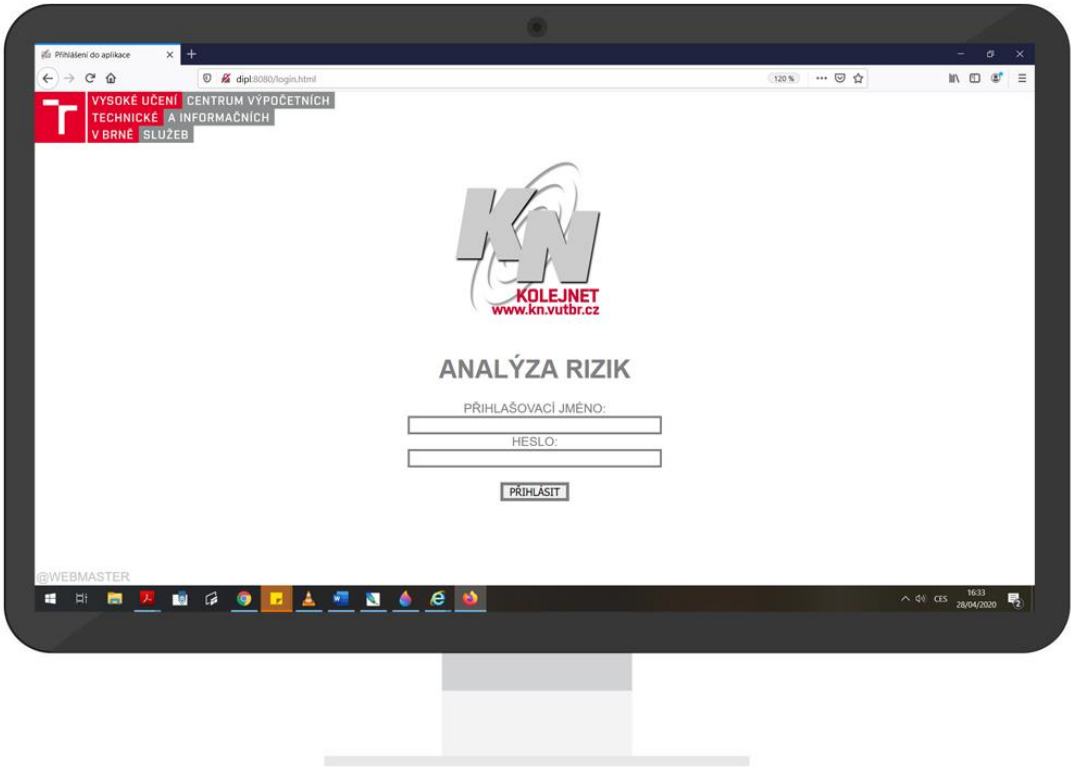
Zobrazení webových stránek bylo testováno ve třech nejpoužívanějších webových prohlížečích – Google Chrome, Mozilla Firefox a Internet Explorer. Ve všech prohlížečích se text (včetně kódování) i barvy zobrazovaly správně. V některých případech zobrazoval Internet Explorer prvky, které nepodporoval v použité verzi, jinak pozicované.



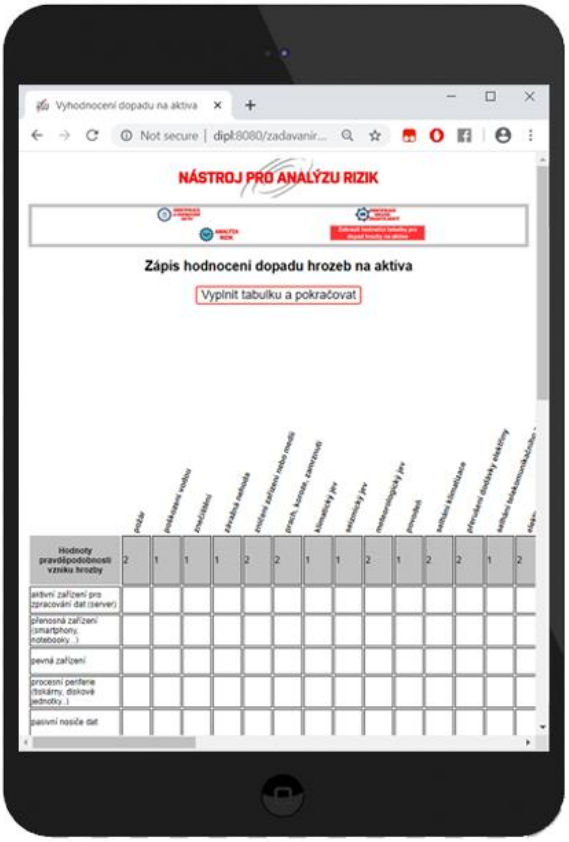
Obrázek 47: zobrazení v prohlížeči Google Chrome (Vlastní zpracování)



Obrázek 48: zobrazení v prohlížeči Internet Explorer (Vlastní zpracování)



Obrázek 49: zobrazení v prohlížeči Mozilla Firefox (Vlastní zpracování)



Obrázek 50: zobrazení na přenosném zařízení (Vlastní zpracování)

4.8. Finanční ohodnocení projektu

Pro kalkulaci nákladů na vývoj, zavedení i provoz nepoužijeme žádnou z běžných metod kalkulace nákladů jako kalkulaci přirážkovou, kalkulaci dělením či rozdílovou kalkulaci, protože jejich parametry jsou pro tento projekt nevhodné. [18] Pro definovaní nákladových tabulek využijeme odhadované částky nákladů. Mzdové náklady se budou odvíjet o statistických dat získaných na webu Českého statistického úřadu. V roce 2019 činila průměrná hrubá mzda 31 125 Kč za měsíc, to v přepočtu na hodinový výdělek odpovídá téměř 200 Kč za hodinu. Pro zjednodušení výpočtu budeme tuto přibližnou hodnotu i nadále používat. Fixní náklady za energie a služby se s provozem aplikace nezvýší, nejsou proto uvažovány do výpočtů nákladové tabulky. Nepřímé neboli režijní náklady zahrnují v tomto případě různé prvky správní režie, tedy náklady na řízení, plánování a kontrolu provozu a činností v oddělení. Jednotlivé fáze a jejich nákladové položky jsou rozepsány v souladu s WBS projektu. Jejich odhadované doby trvání

vymezují právě alespoň minimální časovou dotaci pro jednotlivé činnosti a k tomu přepočtené příslušné mzdové náklady. Nejvyšší nákladové položky jsou samotný vývoj a následné monitorování provozu či průvodní sběr dat a sestavení pragmatické analýzy. Celkové náklady jsou téměř 500 000 Kč, protože se jedná o velice vysokou částku, samotné realizaci projektu musí předcházet konzultace a schválení vývoje a zavedení aplikace vedením.

Tabulka 10: náklady spojené s vývojem a provozem aplikace (Vlastní zpracování)

fáze	název nákladu	odhadovaná doba trvání (měsíců)	ve dnech	lidské zdroje (cena za jednotku)	lidské zdroje (cena celkem)	energie a služby (celkem)	režijní náklady (celkem)	*CELKEM (rok)*
1.1	Sběr dat	1	30	200.00	48,000.00		5,000.00	53,000.00
1.2	Pragmatická analýza rizik	1	30	200.00	48,000.00			48,000.00
2.1	Příprava infrastruktury	0.1	3	200.00	4,800.00	stávající fixní náklad		4,800.00
2.2	Příprava prostředí	0.2	6	200.00	9,600.00	stávající fixní náklad		9,600.00
3.1	Vývoj	4	120	200.00	192,000.00		2,000.00	194,000.00
3.2	Testování	0.5	15	200.00	24,000.00		1,000.00	25,000.00
4.1	Zavádění - organizační změny	0.2	6	200.00	9,600.00		2,000.00	11,600.00
4.2	Zavádění - HW a SW	0.1	3	200.00	4,800.00	stávající fixní náklad		4,800.00
4.3	Zavádění - dokumentace	0.1	3	200.00	4,800.00		1,000.00	5,800.00
4.4	Zavádění - školení personálu	0.5	14	200.00	22,400.00		1,000.00	23,400.00
5.1	Spuštění do provozu	0.04	1	200.00	1,600.00	stávající fixní náklad		1,600.00
5.2	Monitorování	12	360	monitorovací systém		stávající fixní náklad	60,000.00	60,000.00
5.3	Přezkoumání	0.5	15	200.00	24,000.00		1,000.00	25,000.00
					roční náklad	celkem za vstupní analýzy		*101,000.00*
						celkem za vývoj		*233,400.00*
						celkem za integraci		*45,600.00*
						celkem za provoz		*86,600.00*
						CELKEM		***466,600.00***

ZÁVĚR

Cílem této práce bylo navrhnout webovou aplikaci na analyzování rizik a usnadnit a urychlit tak procesy a činnosti spojené s touto problematikou. Zásadní požadavek je konzistentnost aplikace s již provozovaným informačním systémem, neboť ten tvoří jádro obchodní činnosti oddělení, a jednoduchost při obsluze i zpracování dat. Účelem je efektivní a rychlé vyhodnocování analýzy a akční rozhodování spíše, než komplikované strategické plány na několik let dopředu. Vzhledem ke své konstrukci však může být aplikace pojata obecněji a přizpůsobena i výrazným změnám.

Teoretické poznatky posloužily jako základní stavební kámen pro návrhovou část i pro komplexnější pochopení problematiky. Vazby mezi jednotlivými částmi práce jsou zřejmé, a proto bylo vhodné tímto způsobem také uvažovat při řešení této práce.

Na základě analýz jsme vyhodnotili, že aplikace bude dobře využitelná, a prostředí oddělení je připravené pro její integraci, ať už jako součást systému řízení bezpečnosti informací nebo samostatně.

Návrhová část představuje webovou aplikaci jako nový pracovní nástroj, se kterým ale není spojen pouze vývoj a testování, ale také integrace do prostředí a organizační struktury, nová dokumentace a školení zaměstnanců. Tedy mnoho dalších úkonů, které bychom neměli opomenout, proto bylo na práci nahlíženo ve všech kapitolách komplexněji.

SEZNAM POUŽITÉ LITERATURY

[1] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice.* Brno: CERM, 2013, 377 s. grafy, tab.
ISBN 978-80-7204-872-4.

[2] JORDÁN, Vilém. *Infrastruktura komunikačních systémů II: kritické aplikace*. Brno: Akademické nakladatelství CERM, 2015, 232 s. : il..
ISBN 978-80-214-5240-4.

[3] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o, 2016, 522 stran : il..
ISBN 978-80-88168-15-7.

[4] ČSN ISO/IEC 27000 (36 9797) *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014, 25 s. : il., tab.

[5] ČSN ISO/IEC 27001 (36 9790) *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010, 23 s. : il., tab.

[6] ČSN ISO/IEC 27005 (36 9790*) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Řízení rizik bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013,
64 s. : il., tab.

[7] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. : portréty, grafy, tab. ISBN 978-80-7431-050-8.

[8] CENTRUM VÝPOČETNÍCH A INFORMAČNÍCH SLUŽEB. *O nás*. [online] Brno: Vysoké učení technické v Brně, 2019. [cit. 19-12-2019]. Dostupné z: https://www.vutbr.cz/cvis

[9] VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ. *Profil univerzity.* [online] Brno: Vysoké učení technické v Brně, 2019. [cit. 19-12-2019]. Dostupné z: https://www.vutbr.cz/

[10] CESNET. *Spolupráce.* [online] Praha: CESNET, 2018. [cit. 06-01-2020]. Dostupné z: https://csirt.cesnet.cz/cs/cooperation

[11] PROCHÁZKA, David. *PHP 6: začínáme programovat*. Praha: Grada, 2012, 183 s. : il.. ISBN 978-80-247-3899-4.

[12] VRÁNA, Jakub. *1001 tipů a triků pro PHP*. Brno: Computer Press, 2010, 456 s. : il. + 1 CD-ROM. ISBN 978-80-251-2940-1.

[13] MCKINSEY & COMPANY. *McKinsey Quarterly*. [online] New York: McKinsey & Company, 2008. [cit. 06-01-2020]. Dostupné z: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/enduring-ideas-the-7-s-framework#

[14] RAIS, Karel a Radek DOSKOČIL. *Risk management: studijní text pro kombinovanou formu studia*. Brno: Akademické nakladatelství CERM, 2007, 152 s. : il. ISBN 978-80-214-3510-0.

[15] KOCH, Miloš. [online] *ZEFIS online systém pro posouzení efektivnosti informačních systémů.* [cit. 06-01-2020]. Dostupné z: https://www.zefis.cz/

[16] GUINN, Alan, Oldřich KRATOCHVÍL a Iveta HASHESH. *Strategický management.* Kunovice: Evropský polytechnický institut, 2007. s. 59. ISBN 978-80-7314-125-7. Dostupné také z: https://kramerius5.nkp.cz/uuid/uuid:24ac5e88-1b01-4441-a9aa-e6423b9806f8

[17] MARIADB FOUNDATION. [online] *About.* [cit. 06-01-2020]. Dostupné z: https://mariadb.org/

[18] SYNEK, Miloslav. *Manažerská ekonomika.* Praha: Grada, 2011. s. 104. ISBN 978-80-247-3494-1. Dostupné také z: https://kramerius5.nkp.cz/uuid/uuid:001dcbe0-5096-11e9-918e-5ef3fc9ae867

[19] WORLD WIDE WEB CONSORTIUM. [online] *About W3C.* [cit. 06-01-2020]. Dostupné z: https://www.w3.org/Consortium/

[20] MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. [online]. *Statistika školství.* [cit. 06-01-2020]. Dostupné z: http://www.msmt.cz/vzdelavani/skolstvi-v-cr/statistika-skolstvi

[21] SCHWALBE, Kathy. *Řízení projektů v IT: kompletní průvodce*. Brno: Computer Press, 2011, 632 s. : il. ISBN 978-80-251-2882-4.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHY

Příloha 1: návrh metodiky řízení rizik (Vlastní zpracování)

Čj.: XYZ/0000/00
V Brně, dne DD.MM.RRRR
Rozdělovník: XYZ
Zpracoval: XYZ

Směrnice č. 00/0000

NÁVRH METODIKY ANALÝZY RIZIK

Článek 1
Základní ustanovení

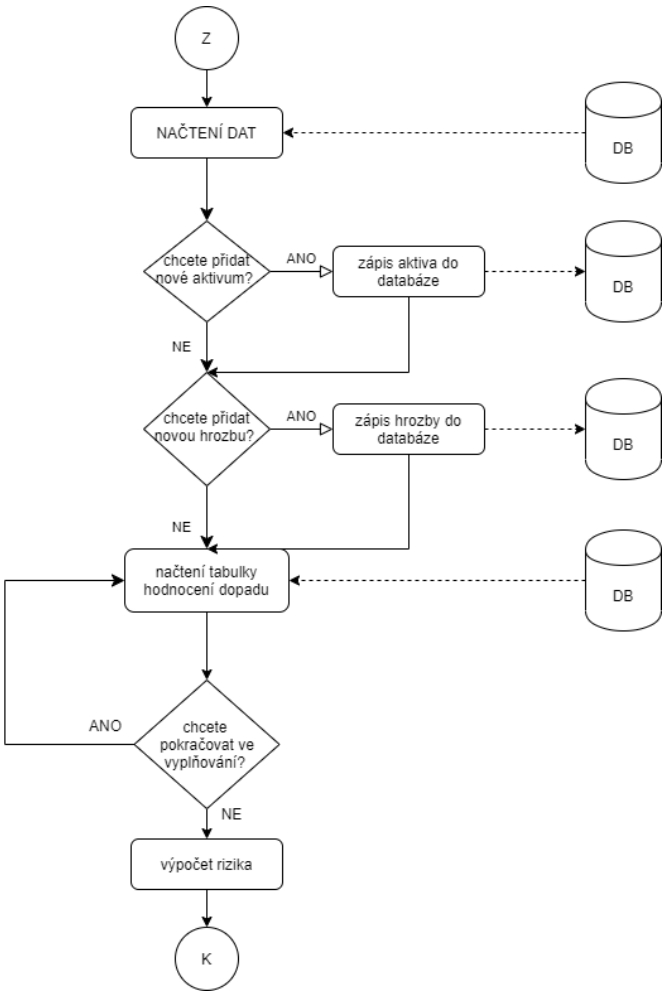
1. Metodika dokumentuje postup analýzy rizik v organizaci, je závazná pro všechny zúčastněné strany, především pro zaměstnance na všech úrovních řízení.
2. Je vedena formou dokumentu, jako vnitřní předpis.
3. Kontrolu, monitorování a úpravy provádí pověřená osoba jedenkrát za rok.
4. Pravidelná analýza rizik se provádí na předem definované oblasti, pomocí předem definovaných kritérií a je prováděna pověřenou osobou, v rámci revize řízení rizik.
5. Výsledky analýzy rizik jsou předávány vedení k projednání.

Článek 2
Diagram postupu analýzy rizik

1. Metodika určuje pomocí digramu postupu, proces analýzy rizik v oddělení.
2. Diagram postupu je obecný a může být modifikován pro aktuální potřeby oddělení.
3. Začátek procesu je označen kruhovým prvkem Z a konec procesu je označen kruhovým prvkem K, kosočtverce označují rozhodovací bloky a obdélníkové bloky označují činnosti.
4. K provádění postupu slouží webová aplikace, umístěná v IS.
5. S webovou aplikací pracuje pověřená osoba, obsluha aplikace v pravidelném intervalu (jednou za 12 měsíců při revizi) a v případě, že je aktualizace dat potřeba.

6. Výsledky z aplikace se reportují nadřízenému pracovníkovi bezpečnosti.

Proces analyzování rizik – diagram:



Článek 3
Hodnotící tabulky

1. Hodnotící tabulky slouží pro správné vyhodnocení analýzy a využijeme je při hodnocení integrity, důvěrnosti, dostupnosti a dopadu v případě analýzy aktiv. Dále také při hodnocení hrozeb a pravděpodobnosti jejich vzniku, a také při určování dopadu hrozeb na jednotlivá aktiva.
2. K hodnocení se vždy využívají následující tabulky se stupnicemi. Tyto tabulky lze upravovat pouze při významných změnách v organizaci.
3. Hodnocení rizik slouží zejména pro prioritizaci rizik a následné volbě opatření.
4. Hodnotíme pomocí číselných hodnot, pouze v případě hodnocení pravděpodobnosti vzniku hrozby hodnotíme slovně.

Hodnocení HW aktiv:

Pořízení nového HW	Dopad při přerušení činnosti
1 = zanedbatelná cena	1 = zanedbatelná hodnota
2 = cena do 25.000 Kč	2 = velmi nízká
3 = cena 25.000-50.000 Kč	3 = nízká
4 = cena 50.000-100.000 Kč	4 = střední
5 = cena 100.000-250.000 Kč	5 = vysoká
6 = cena 250.000-1.000.000 Kč	6 = velmi vysoká
7 = cena nad 1.000.000 Kč	7 = kritická

Hodnocení SW aktiv:

Pořízení nové licence/nový vývoj open source	Dopad při přerušení činnosti
1 = zanedbatelná cena	1 = zanedbatelná hodnota
2 = cena do 25.000 Kč	2 = velmi nízká
3 = cena 25.000-50.000 Kč	3 = nízká
4 = cena 50.000-100.000 Kč	4 = střední
5 = cena 100.000-250.000 Kč	5 = vysoká
6 = cena 250.000-1.000.000 Kč	6 = velmi vysoká
7 = cena nad 1.000.000 Kč	7 = kritická

Hodnocení informačních aktiv:

Porušení zákona a dobrého jména	Dopad při přerušení činnosti, porušení aktiva
1 = bez dopadu, veřejná informace	1 = zanedbatelná hodnota
2 = bez dopadu, neveřejná informace	2 = velmi nízká
3 = pravděpodobně neovlivní společnost	3 = nízká
4 = ovlivní společnost	4 = střední
5 = porušení triády AAA, finanční dopad na společnost v hodnotě do 100.000 Kč	5 = vysoká
6 = porušení triády AAA, finanční dopad na společnost v hodnotě více jak 100.000 Kč a méně než 1.000.000 Kč	6 = velmi vysoká
7 = vysoký dopad na společnost v hodnotě více jak 1.000.000 Kč	7 = kritická

Hodnocení aktiv lidských zdrojů:

Ztráta zaměstnance - riziko	Potenciál poškození
1 = nulová praxe a nízké investice do školení	1 = zanedbatelný
2 = nulová praxe a investice do školení do 25.000 Kč	2 = velmi nízký
3 = nulová praxe a investice do školení 25.000-50.000 Kč	3 = nízký
4 = praxe 1 rok v oboru a nízké investice do školení	4 = střední
5 = praxe 1 rok v oboru a investice do školení do 50.000 Kč	5 = vysoký
6 = praxe více jak 1 rok v oboru a investice do školení do 50.000 Kč	6 = velmi vysoký
7 = praxe více jak 3 roky v oboru a investice do školení nad 50.000 Kč	7 = kritický

Hodnocení pravděpodobnosti vzniku hrozby:

Úroveň (pravděpodobnost)	Popis (hodnota)
malá	1
střední	2
velká	3

Hodnocení dopadu hrozeb na aktiva:

Dopad hrozby	Hodnota	Popis
Fatální	5	**Kompletní zničení a následující úplná obnova, včetně infrastruktury**
Kritický	4	**vážné požkození a následující obnova (náklady > 1 mil Kč)**
Střední	3	**velké požkození a následující obnova (náklady > 100 000 Kč)**
Nízký	2	**požkození a následující obnova (náklady > 10 000 Kč)**
Zbytkový	1	**drobné nebo nevýznamné požkození**

Hodnocení a prioritizace rizik:

Úroveň	hodnota	Popis
Významné riziko	>=10	Riziko nelze akceptovat, naopak využijeme plán zvládání rizik a implementujeme opatření v co nejkratším čase.
Přijatelné riziko	5-9	Riziko lze akceptovat v případě, že jsou náklady na řízení rizika neúměrně vysoké oproti způsobeným škodám.
Nevýznamné riziko	1-4	Není nutné nasazovat opatření, riziko můžeme akceptovat.

Článek 4
Katalog hrozeb

5. Pro základní katalog hrozeb je jako zdroj použita a případně modifikována příloha C, normy ČSN ISO/IEC 27 005.
6. Zdroje rozdělujeme na N -náhodné, Ú – úmyslné, a E – enviromentální.
7. Katalog hrozeb může být v aplikaci doplněn o další hrozby s možným působením na oddělení.
8. Při vkládání nové hrozby musí být v aplikaci vyplněna všechna pole.

Katalog hrozeb 1. část:

Typ	Hrozby	Zdroj
Fyzické poškození	Požár	N, Ú, E
	Poškození vodou	N, Ú, E
	Znečištění	N, Ú, E
	Závažná nehoda	N, Ú, E
	Zničení zařízení nebo médií	N, Ú, E
	Prach, koroze, zamrznutí	N, Ú, E
Přírodní události	Klimatický jev	E
	Seizmický jev	E
	Meteorologický jev	E
	Povodeň	E

Katalog hrozeb 2. část:

Typ	Hrozby	Zdroj
Ztráta základních služeb	Selhání klimatizace nebo dodávky vody	N, Ú
	Přerušení dodávky elektřiny	N, Ú, E
	Selhání telekomunikačního zařízení	N, Ú
Poruchy způsobené zářením	Elektromagnetické záření	N, Ú, E
	Termální záření	N, Ú, E
	Elektromagnetické impulzy	N, Ú, E
Ohrožení informací	Zachycení kompromitujících interferenčních signálů	Ú
	Vzdálená špionáž	Ú
	Odposlech	Ú
	Krádež médií nebo dokumentů	Ú
	Krádež zařízení	Ú
	Zprovozněni recyklovaných nebo vyřazených médií	Ú
	Vyzrazení	N, Ú
	Data pocházející z nedůvěryhodných zdrojů	N, Ú
	Falšování pomocí technického vybavení	Ú
	Falšování pomocí aplikačního programového vybavení	N, Ú
	Odhalení pozice	Ú

Katalog hrozeb 3. část:

Typ	Hrozby	Zdroj
Technická selhání	Selhání zařízení	N
	Chybné fungování zařízení	N
	Přetížení informačního systému	N, Ú
	Chybné fungování aplikačního programového vybavení	N
	Chyba údržby	N, Ú
Neoprávněné činnosti	Neoprávněné použití zařízení	N
	Podvodné kopírování aplikačního programového vybavení	N
	Použití padělaného nebo zkopírovaného aplikačního programového vybavení	N, Ú
	Poškození dat	N, Ú, E
	Nezákonné zpracování dat	N, Ú, E
Ohrožení funkčnosti	Chyba v používání	N, Ú, E
	Zneužití oprávnění	N, Ú, E
	Falšování práv	N, Ú, E
	Odepření činností	N, Ú, E
	Nedostatek personálu	N, Ú, E