VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

MANAGEMENT BEZPEČNOSTI INFORMAČNÍCH SYSTÉMŮ V OBCI

SECURITY MANAGEMENT OF INFORMATION SYSTEMS FOR THE KALIŠTĚ MUNICIPALITY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. PAVEL KUTIŠ
AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák
SUPERVISOR

BRNO 2013

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2012/2013
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Kutiš Pavel, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Management bezpečnosti informačních systémů v obci

v anglickém jazyce:

Security Management of Information Systems for the Kaliště Municipality

Pokyny pro vypracování:

Osnova zadání:
Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současná situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Požadavky. Praha: Český normalizační institut, 2006.
ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Soubor postupů. Praha: Český normalizační institut, 2008.
DOUCEK P., L. NOVÁK a V. SVATÁ Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.
KNÝ, M. a J. POŽÁR Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti. Brno: Tribun EU, 2010. ISBN 978-80-7399-067-1.
POŽÁR, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-3¬8-5.

Vedoucí diplomové práce: Ing. Petr Sedlák

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2012/2013.

L.S.

doc. RNDr. Bedřich Půža, CSc.	doc. Ing. et Ing. Stanislav Škapa, Ph.D.
Ředitel ústavu	Děkan fakulty

V Brně, dne 20.05.2013

Abstrakt

Tato diplomová práce je zaměřena na zavedení managementu bezpečnosti informačních systémů v obci. Práce je rozdělena na dvě hlavní části. V první části jsou sepsána teoretické východiska, která jsou převážně čerpána z norem řady ISO/IEC 27000. V druhé části jsou teoretické poznatky využity pro zavedení managementu informačních systémů v obci. Toto zavedení je rozděleno na tři fáze a podrobně je v práci popsána první fáze.

Abstract

This Diploma Thesis is being focused on Information Security Management System implementation for a certain municipality. The work has been divided into two parts. The first part deals with theoretical basis which are based on the ISO/IEC 27000 standards. The second part contains the practical implementation following the theoretical background from the first part. The implementation itself has been divided into three stages and this thesis is mainly concentrated on the first stage.

Klíčová slova

Management bezpečnosti informačních systémů, obec, riziko, aktivum, opatření, normy řady ISO/IEC 27000

Keywords

information security management system, municipality, risk, asset, control, standards of ISO/IEC 27000

Bibliografická citace práce:

KUTIŠ, P. *Management bezpečnosti informačních systémů v obci*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2013. 77 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Čestné prohlášení

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

V Brně dne 21. května 2013

……

Bc. Pavel Kutiš

Poděkování

Zde bych rád poděkoval svému vedoucímu Ing. Petru Sedlákovi za odborné rady a cenné připomínky, které přispěly ke kvalitnímu vypracování této diplomové práce. Dále bych rád poděkoval své rodině, přítelkyni a přátelům za podporu při celé délce mého studia. Rovněž bych rád poděkoval zaměstnancům obecního úřadu za ochotné předávání informací a kvalitní spolupráci.

Obsah

1 Úvod

S rozvojem výpočetní techniky se stále více informací ukládá právě ve výpočetní technice. Proto je nutné, aby tato technika byla dobře zabezpečena a informace byly poskytovány pouze oprávněným osobám.

Data ve výpočetní technice jsou dostupná velkému počtu uživatelů této techniky a díky připojení pracovních stanic do celosvětové počítačové sítě jsou data rovněž dostupná i okolnímu světu.

Díky propojení s celosvětovou počítačovou sítí jsou kladeny vysoké nároky na zabezpečení dat. Informace dnes můžeme považovat za to nejdůležitější, co lze v podniku nebo v jiné organizaci nalézt. Této hodnoty informací jsou si vědomi i osoby, které chtějí informace získat. K získání informací se nebojí použít i nelegálních a neetických prostředků. Velmi často se v médiích vyskytují zprávy o útocích na různé organizace.

Nejčastějším cílem útoků bývá zjištění informací o vyvíjených technologiích, o nových výrobcích, o osobních datech, nebo získání finančních prostředků organizace. Pokud se útočníkům jejich záměr podaří, je to pro podnik vždy vážná ztráta, někdy to dokonce vede k existenčním problémům organizace.
Aby bylo zabráněno takovýmto škodám, které útočníci mohou napáchat, většina organizací investuje do zabezpečení informačních systémů značné finanční prostředky.

Zabezpečení informací a dat není jednoduchý proces. Neustále vznikají nová rizika, na která je třeba reagovat. Proto proces zabezpečování nikdy nekončí. Je nutné zabezpečit nejen výpočetní techniku, ale rovněž i fyzickou ochranu budov a proškolit vlastní personál. V tomto procesu zabezpečování lze využít postupy, které byly časem ověřeny a jsou uvedeny v managementu informační bezpečnosti.

Tato práce je rozdělena na dvě hlavní části. První část popisuje základní složky bezpečnosti informačních systémů a metodické pokyny pro zavádění managementu informační bezpečnosti v organizaci. Ty jsou čerpány z řady norem ISO/IEC 27000.
Druhá část práce využívá poznatků z první části a aplikuje je na zavedení ISMS do obce. V této části je hlavně popsána realizace zvolených opatření z norem tak, aby se snížily dopady rizik a zvýšila se bezpečnost informací ve zvolené obci.

2 Vymezení problému a cíle práce

Diplomová práce se zaměřuje na řešení managementu informační bezpečnosti v malé obci. Každá obec má některé záznamy, které nejsou veřejně přístupné a měl by k nim mít přístup pouze zaměstnanec se správným oprávněním. Jde například o ochranu osobních údajů občanů obce, která je dána ze zákona.
Bezpečnost informací nezahrnuje pouze zabezpečení zařízení, kde jsou chráněná data uložena, ale jde i o zabezpečení celých budov a poučení vhodných osob, kteří s daty pracují.

Cílem této diplomové práce je zanalyzovat současný stav bezpečnosti informací a vypracovat metodiku zavedení ISMS pro zvolenou obec z informací získaných především z řady norem ISO/IEC 27000. Dále jde o popsání realizace konkrétních návrhů na opatření proti zjištěným rizikům a ekonomicky zhodnotit náročnost zavedení opatření.

3 Teoretická východiska práce

3.1 Obecné pojmy informační bezpečnosti

Při řešení managementu informační bezpečnosti je nutné se nejprve seznámit s dále uvedenými výrazy. Tyto výrazy jsou pro někoho jistě známé, ale je třeba, aby byly chápány ve správném smyslu.

- Systém – systém je účelové definování množin prvků P_x a množin vazeb $R_{x,y}$, které jsou mezi prvky. Společně množina prvků a vazeb určuje vlastnosti celého systému. (1)
- Aktivum (Asset) – může být cokoli v organizaci, co pro ni má nějakou hodnotu. Aktiva můžeme v oblasti IS/ICT dělit na:
    - Hmotná aktiva – jsou to především technické prostředky výpočetní techniky (počítače, modemy, tiskárny, kabelové rozvody…).
    - Nehmotná aktiva – to jsou pracovní postupy, data, programové vybavení a služby.

Z pohledu oblasti řízení bezpečnosti informací a ISMS se aktiva dělí na:

- Primární aktiva – převážně nehmotná aktiva (informace), funkční procesy a aktivity organizace, znalosti a know-how.
- Sekundární aktiva – převážně hmotná aktiva jako technické vybavení, komunikační infrastruktura, programové vybavení, prostory i např. pracovníci.

- Hrozba (Threat) – případná příčina nechtěného incidentu, která může poškodit systém nebo organizaci. Hrozbou může být také zneužití zranitelnosti. Hrozby můžeme rozdělit na:
    - přírodní a fyzické – živelné pohromy a nehody (požár, povodeň, výpadek dodávky elektrického proudu…)
    - technické a technologické – poruchy nosičů dat, sítí, poruchy programové atd.
    - lidské – ty se dále člení na neúmyslné a úmyslné (zvenčí systému nebo zevnitř)

Více jak 50 % hrozeb patří do kategorie neúmyslných hrozeb a až 98 % jsou hrozby vnitřní. (2)

- Opatření (Control) – je technika, postup, zařízení nebo aktivita, která snižuje dopady hrozby nebo ji zcela eliminuje.
- Zranitelnost (Vulnerability) – jedná se o slabé místo aktiva nebo opatření, které může být zneužito hrozbou.
- Riziko (Risk) – jde o kombinaci hrozby a zranitelnosti aktiva, případně ještě provedených opatření spojených s daným aktivem.
- Dopad (Impact) – nepříznivá událost vzniklá na aktivu vlivem hrozby. (3)

3.2 Důležitost bezpečnosti

V dnešní době musí organizace, ať už územní samosprávné celky, nebo firmy zpracovávat velké množství informací. Tyto informace se přesouvají z papíru do elektronické podoby a jsou mnohdy nejcennějším aktivem, jaké organizace vlastní. U firem to může být know-how, na kterém je firma založena a v případě jeho vyzrazení by ztratila svou konkurenční výhodu. V případě obcí jde např. o utajení osobních dat občanů obce. (4)

Narůstáním množství informací se rozvinula potřeba vylepšovat systémy na zpracování těchto dat a následně data správně analyzovat, vyhodnotit a využít.

V minulosti se informační bezpečnosti věnovaly jen státní organizace zaměřené na bezpečnost a utajení strategických rozhodnutí. Postupem doby se informační bezpečnost rozšířila i do běžného užívání. V některých případech je bezpečnost informací dokonce vyžadována, jde například o komunikaci státní správy a firem, které se chtějí podílet na státních zakázkách a bez splnění požadavků bezpečnosti nemají možnost zakázku získat. (2)

Oblast informační bezpečnosti je značně rozsáhlá. Jsou v ní zahrnuty faktory, které by mohly umožnit nepovoleným osobám získat důvěrné informace. Je důležité, aby byly informace chráněny v průběhu všech etap jejich zpracování. Současně se musí zachovat jejich přístupnost osobám povoleným. V organizaci by měla být tedy provedena taková opatření, která zabezpečí i ty běžné činnosti, jako je např. zálohování.

V České republice je informační bezpečnost ještě stále velmi podceňována. Situace se postupem času zlepšuje. Největší problém v informační bezpečnosti jsou samozřejmě finance. Vedení organizací si většinou neuvědomuje důsledky, které mohou vzniknout nevytvářením informační bezpečnosti. Finanční prostředky v organizaci jsou mnohdy omezené, a tak na informační bezpečnost nevystačují. Informační bezpečnosti ani moc nenapomáhají zákony v České republice. Těmi jsou upravena pouze některá hlediska, jako je ochrana osobních údajů a neřeší informační bezpečnost jako celek. Z principu ani nemohou, protože každá organizace je jiná a nelze tedy stanovit, co má a co nemá být zabezpečeno. Jen samotná organizace ví, jaká aktiva jsou pro ni nejdůležitější.

V některých organizacích, kde jsou informace velmi důležité, je můžeme považovat za další zdroj ke zdrojům lidským, kapitálovým a výrobním. Tyto informační zdroje dokonce někdy převažují a tvoří hlavní aktiva firmy. Aby si organizace tyto zdroje mohla optimálně chránit, je nutné informační zdroje ocenit dle jejich důležitosti a nežádoucího dopadu na chod organizace. (5)

Informační bezpečnost tedy nemá v organizaci stanoveno jedno přesné řešení. Každá organizace si ji musí vytvořit samostatně. Aby to pro organizaci nebylo tak složité, byly vytvořeny návody, doporučení a mechanismy, jak tuto problematiku vyřešit. Informační bezpečnost s sebou přináší i řadu dalších oblastí, které je nutné vyřešit. Jde například o fyzickou bezpečnost, která zahrnuje přístup do budov, přístup k zařízením, kabelovému propojení mezi počítači atd. Dále je to oblast dostupnosti dat, jejich zálohování, ochrana počítačů před škodlivými kódy, šifrování dat, řešení situace v případě poruchy atd. Další oblastí je dodržování směrnic, analýza možných rizik, proškolování zaměstnanců atd. Jak je vidět, informační bezpečnost v sobě zahrnuje mnoho dalších oblastí, které by se měly zabezpečit. (6)

Zabezpečení všech oblastí, které jsou spojeny s řízením bezpečnosti informací, vyžaduje poměrně rozsáhlé investice. Proto je tato oblast některými organizacemi zanedbávána. Dále je uvedeno několik důvodů, proč řešit bezpečnost informací.

- Zavedením ISMS se do organizace vnese bezpečnostní politika. Ta určuje, jak má být organizace nejlépe chráněna před vnějšími útoky. Díky tomu se velmi snižuje riziko úniku důležitých dat a jejich zneužití.

- Při zavedení ISMS se ohodnotí aktiva a díky tomu jsou zavedena pouze taková opatření, která jsou nutná. Jsou tak ušetřeny a efektivně využity finanční prostředky.
- Po zavedení ISMS jsou také stanoveny mechanismy, které popisují způsob řešení neočekávaných událostí a hledání nových vzniklých rizik, pro která jsou vytvořena návrhy řešení. Díky tomuto cyklu se ISMS v organizaci stále zlepšuje a odpovídá více realitě.
- V současnosti se mnoho organizací zaměřuje na získání certifikátu managementu jakosti dle normy ISO 9000. Je to jistě konkurenční výhoda. Podobné výhody může dosáhnout firma i zavedením managementu bezpečnosti informačních systémů dle normy ISO 27000.
- Pracovníci jsou rozděleni do skupit podle vykonávané činnosti a mají nastavena přístupová práva pouze k výkonu své práce. Zvyšuje se tak efektivnost práce, protože nemohou využívat jiných služeb, které by je zpomalovaly v jejich práci.

3.3 Informační bezpečnost

Informační bezpečnost je systém ochrany dat a informací. Tyto informace, nebo data se mohou vyskytovat při vstupu, zpracování, ukládání, přenosu a jejich smazání.

Existují různá opatření, kterými lze data a informace chránit. Jsou to opatření logická, technická programová a organizační. Díky těmto opatřením by se mělo zamezit ztrátě důvěrnosti, integrity a dostupnosti[1]. (7)

Bezpečnost nebude nikdy stoprocentní, proto je nutné, aby jednotky vždy počítaly s jakousi mírou rizika, která pro ně bude akceptovatelná.

3.4 Cíle informační bezpečnosti

Informační bezpečnost má stanoveny cíle, které norma ISO/IEC 27001 rozděluje následovně:

Důvěrnost – informace jsou přístupné pouze uživatelům, kteří k nim mají mít umožněn přístup.

Dostupnost – informace by měla být na vyžádání vždy dostupná uživatelům s přístupem.

Integrita – zajišťuje, aby informace zůstala celistvá a neměnná.

[1] Tyto pojmy jsou vysvětleny v další kapitole

3.5 Bezpečnost informací

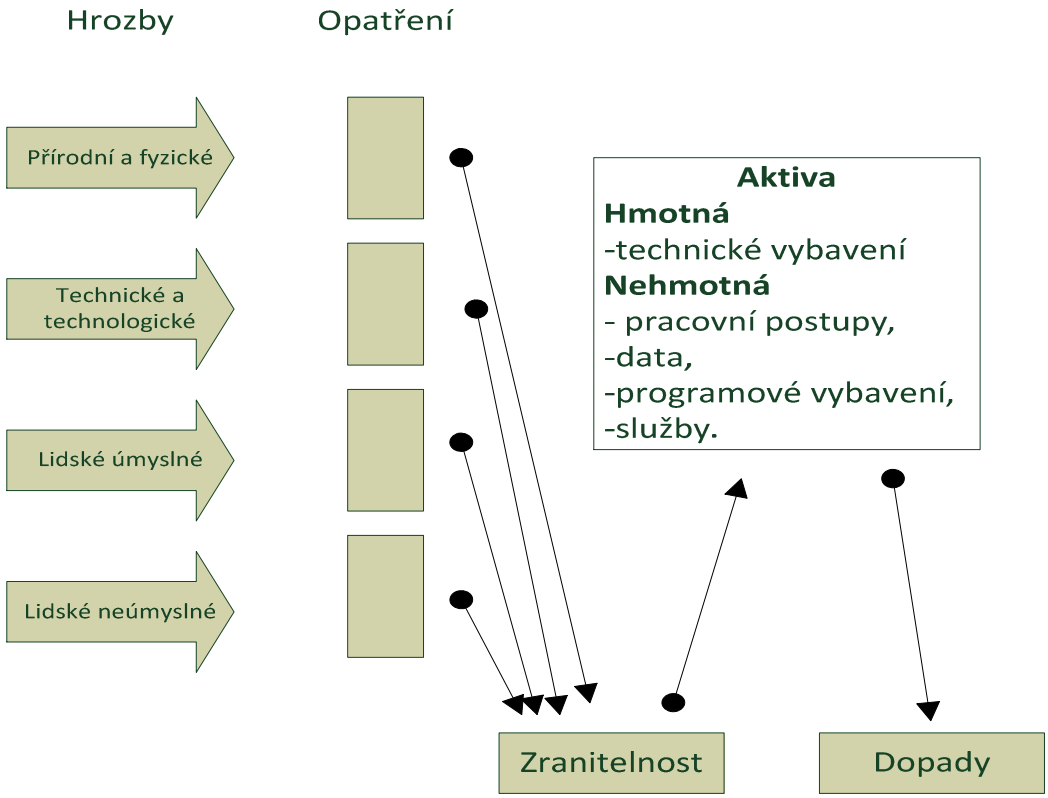
Abychom mohli dobře pochopit bezpečnost informací, je nutné chápat i návaznost tohoto pojmu na bezpečnost organizace a bezpečnost IS/ICT.

Bezpečnost organizace zahrnuje bezpečnost objektu, majetku organizace a v neposlední řadě i bezpečnost informací. Napomáhá rovněž k bezpečnosti IS/ICT a to tím, že se např. kontroluje fyzický přístup do objektů společnosti.

Bezpečnost informací zahrnuje veškeré činnosti, které se týkají práce s informacemi. Jde o informace všech typů, tedy i o informace v nedigitální podobě. V bezpečnosti informací se řeší např. zpracování dat, jejich uložení, způsoby skartace, činnosti nutné během přesouvání informací atd.

Bezpečnost IS/ICT je součástí bezpečnosti informací a je zaměřena na chránění aktiv společnosti, která jsou prvky informačního systému ve společnosti. Bezpečnost IS/ICT je tak nejužší oblastí řízení bezpečnosti. (2)

Obrázek 1 Schéma zajištění bezpečnosti IS/ICT v organizaci



Zdroj: Vlastní zpracování (2)

3.6 Normy a zákony v oblasti bezpečnosti IT

Lidé ve svých oborech mají vytvořeny určité postupy, kterými se řídí, aby dosáhli stanoveného cíle. Tyto postupy se zaznamenávají, nebo si je lidé předávají pouze ústní formou. V oboru, který je mezinárodní a zabývá se jím mnoho lidí, je nejlepší možností, jak si předávat informace právě vytvořením psaného postupu, který vede k vytyčenému cíli. Tímto oborem je i management bezpečnosti informačních systémů. Pro něj jsou vytvořeny nadnárodními organizacemi mezinárodní standardy. Organizace, které vytvářejí normy pro bezpečnost informačních systémů, jsou:

- ISO – International Organization for Standardization
- IEEE – The Institute of Electrical and Electronics Engineers
- IEC – International Electrotechnical Comission
- ITU – Internation Telecommunications Union

Vytvořené standardy obsahují přesně definované postupy a usnadňují proces zavedení bezpečnosti informačních systémů. V České republice se standardy berou pouze jako doporučení a nemusíme se jimi řídit a dále jsou zde zákony, kterými se řídit naopak musíme. Je velmi vhodné postupovat i podle standardů, protože se tak zjednoduší možná certifikace managementu bezpečnosti informačních systémů.

3.6.1 Zákony v legislativě České republiky a nařízení EU

V České republice existuje několik zákonů, které jsou s otázkou bezpečnosti informačních systémů nějak spojeny. Současně tak existují i některá nařízení Evropské unie, která se na Českou republiku rovněž vztahují. Popis těchto zákonů by ale zabral v této práci příliš mnoho stran a není zde účelem zákony popisovat, ale brát je v potaz. Proto jsou níže uvedeny nejdůležitější zákony, které mají vliv na praktickou část práce a na bezpečnost informačních systémů v obci.

- **Zákon č. 101/2000 Sb., o ochraně osobních údajů: §1**: *„Tento zákon v souladu s právem Evropských společenství, mezinárodními smlouvami, kterými je Česká republika vázána, a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.“*

§ 3 odst. 1: *„Tento zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby.*“

- **Zákon č. 227/2000 Sb., o elektronickém podpisu §1:** *„Tento zákon upravuje v souladu s právem Evropských společenství používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.“*
- **Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů:** *„Tento zákon vymezuje skutečnosti, které je nutno v zájmu České republiky utajovat, způsob jejich ochrany, působnost a pravomoc orgánů státu při výkonu státní správy v oblasti ochrany utajovaných skutečností, povinnosti orgánů státu, práva a povinnosti fyzických a právnických osob a odpovědnost za porušení povinností stanovených tímto zákonem a upravuje postavení Národního bezpečnostního úřadu.“*
- **Zákon č. 365/2000 Sb. o informačních systémech veřejné správy a jeho novely – zákona č. 81/2006 Sb:** zákon je zaměřen na informační systém veřejné správy, na dlouhodobé řízení informačních systémů veřejné správy, bezpečnost informačních systémů veřejné správy.
- **Vyhláška č. 529/2009 Sb.:** Pojednává: *„o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy*“.
- **Zákon č. 480/2004 Sb. o některých službách informační bezpečnosti:** zákon upravuje odpovědnost a práva a povinnosti osob, které poskytují služby informační společnosti a šíří obchodní sdělení.
- **Nařízení Evropského parlamentu a rady č. 211/2011 o občanské iniciativě**: toto nařízení řeší mimo jiné online systém sběru dat, které se má provádět dle **Prováděcího nařízení komise č. 1179/2011.** V tomto prováděcím nařízení je v příloze uvedeno: *„2.1 Organizátoři předloží dokumentaci, která prokazuje, že splňují požadavky normy ISO/IEC 27001 i bez jejího přijetí.*“ *„2.2 Organizátoři*

si zvolí bezpečnostní kontroly na základě analýzy rizika uvedené v bodě 2.1 písm. a) z těchto norem:

- *1. ISO/IEC 27002 nebo*
- *2. „Zásady řádné praxe“ Fóra informační bezpečnosti“*[2]

3.6.2 ČSN ISO/IEC

ČSN ISO/IEC 27001:2006 popisuje oblasti, které je nutné zvládnout pro zabezpečení a řízení informací v podniku nebo obci. Je určena pro jakoukoli jednotku, která používá externí, nebo interní počítačový systém a pracuje s citlivými daty, která by měla být chráněna (např. rodná čísla občanů obce).

Cílem ČSN ISO/IEC 27001:2006 je zajištění integrity, dostupnosti a důvěrnosti informací. Aby bylo tohoto cíle dosaženo, norma má seznam opatření, kde jsou položky rozděleny do kategorií bezpečnosti a ty dále do seskupených oblastí.

Rozdělení ČSN ISO/IEC 27001:2006		
Oblast	**Počet kategorií**	**Počet opatření**
Akvizice, vývoj a údržba informačních systémů	6	16
Bezpečnost lidských zdrojů	3	9
Bezpečnostní politika	1	2
Fyzická bezpečnost a bezpečnost prostředí	2	13
Organizace bezpečnosti informací	2	11
Řízení aktiv	2	5
Řízení komunikace a řízení provozu	10	33
Řízení kontinuity činností organizace	1	5
Řízení přístupu	7	25
Soulad s požadavky	3	10
Zvládání bezpečnostních incidentů	2	5

Zdroj: norma ČSN ISO/IEC 27001:2006

Splněním požadavků v této normě lze dosáhnout certifikace a následně pak srovnávat např. organizace navzájem. Není ovšem nutné, aby se jednotka zabývala všemi oblastmi, které norma udává. Pro některé jednotky jsou určité oblasti nepodstatné. Proto se vždy nejprve identifikují možné hrozby a ty se pak rozdělí do odpovídajících

[2] Citace jsou převzaty z uvedených zákonů

kategorií. V případě hrozby, která neodpovídá žádné kategorii, je možné do managementu bezpečnosti informačních systémů přidat kategorii novou.

Oblasti, které jsou v normě uvedené, od sebe nelze jednoznačně odlišit. Není tedy ojedinělé, když na sebe oblasti navazují nebo se překrývají. Vypsaný počet opatření v tabulce, který dohromady dává číslo 134, není konečný. Jednotlivá opatření mají několik dalších kroků, které lze brát jako další opatření.

Norma ČSN ISO/IEC 27001:2006 slouží jako příručka, která popisuje praxí ověřený postup řešení určitého problému. Je samozřejmé, že tato norma nemůže obsahovat řešení všech možných problémů, proto se vytváří analýza rizik, na základě které si jednotka sama zvolí, jaké opatření bude zvoleno na daný problém.

3.6.3 Normy ISO/IEC

V roce 1995 byla vytvořena ve Velké Británii norma BS7799 pro oblast bezpečnosti informačních systémů. Tato norma se stala základem pro zavádění managementu bezpečnosti informačních systémů. Během několik let se tato norma rozšířila do dalších zemí a byla označována anglickým názvem Information Security Management Systém – ISMS. V roce 2000 byla norma z roku 1995 přijata jako nadnárodní norma ISO s číslem ISO 17799. Když byla norma z roku 1995 vytvářena, dbalo se na to, aby byla univerzální k mnoha technologiím. To umožnilo její implementaci v různých státech, v různých firmách i v různých samosprávných celcích.

V roce 2005 Mezinárodní organizace pro normalizaci použila normu ISO 17799 pro vytvoření skupiny norem ISO/EIC 27000. Některé části normy ISO 27000 jsou dále popsány.

- ISO 27000 – tato část zavádí definice pojmů a terminologický slovník, které se využívají v dalších částech normy ISO 27000.
- ISO 27001 – tato část normy byla publikována v roce 2005 a je to druhá část původní normy BS7799 vytvořená ve Velké Británii. Je považována za hlavní normu, podle které jsou ISMS certifikovány.
- ISO 27002 – byla označována jako ISO/IEC 17799:2005 a od roku 2007 se její jméno změnilo na ISO/IEC 27002:2005. V této části jsou sepsány nejlepší bezpečnostní praktiky, které lze využít i jako postupy pro docílení bezpečnosti informací v podniku nebo obci.
- ISO 27003 – tato část obsahuje návody pro zavedení ISMS podle ISO 27001.

- ISO 27004 – v této části se nacházejí doporučení pro používání metrik a pro měření účinnosti zavedeného ISMS.
- ISO 27005 – tato část je zaměřena na řízení bezpečnostních rizik informačních systémů.
- ISO 27006 – v této části jsou sepsány požadavky na instituce provádějící certifikaci a audit ISMS.
- ISO 27014 – předností této normy je, že nejlépe vystihuje problematiku veřejné správy a samosprávy a poskytuje doporučení pro vytvoření Information Security Governance. Doporučení zohledňují cíle, strategie, politiky a legislativní povinnosti organizace.[3]

Tento výčet částí norem ISO 27000 není zdaleka úplný. Mnoho lidí, kteří nejsou s problematikou této normy seznámeni, může její množství úseků odradit. Po krátkém prostudování je ale zřejmé, že normy velmi dobře pomáhají s vytvářením bezpečnosti informačních systémů. Malé podniky nebo obce, které nechtějí být certifikovány, nemusí plnit veškeré požadavky, které norma udává. Mohou se zaměřit pouze na nejvíce riziková místa a toto riziko díky normě snížit.

3.7 Integrovaný systém řízení

Integrovaný systém řízení (IMS) je komplexní a průřezový pohled na oblast řízení v organizaci. Pomáhá s realizací základních vazeb mezi jednotlivými odbornými oblastmi řízení. Řízení organizace je proces vnímaný jako řešení komplexního problému, v rámci něhož je nutné řídit organizaci jako celek a také je třeba řídit i všechny dílčí aspekty.

Integrovaný systém řízení je propojením původních jednotlivých autonomních systémů řízení. Dnes se považují za komponenty IMS následující systémy:

- kvalita – Quality Management Systém (QMS)
- vztah k okolí – Environmental Management Systém (EMS)

[3] http://www.rac.cz/rac/homepage.nsf/CZ/ISO27000

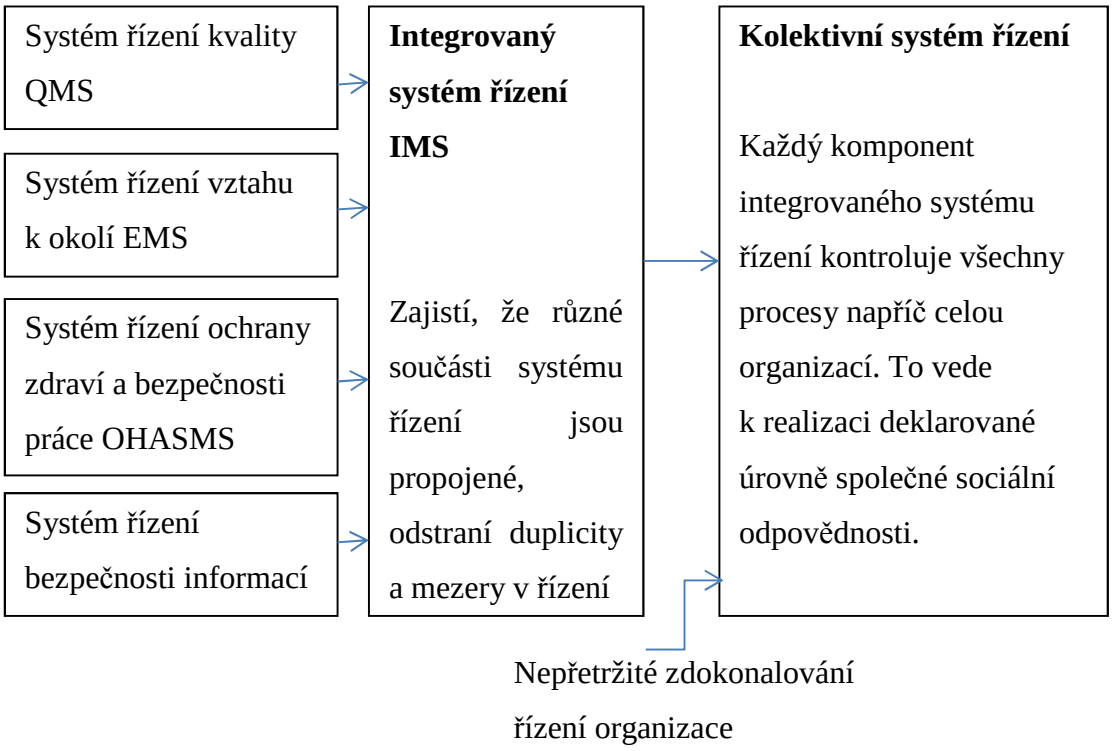
- bezpečnost a ochrana zdraví při práci – Occupational Health & Safety Management Systém (OHASMS), v České republice znám jako BOZP – Bezpečnost a ochrana zdraví při práci
- bezpečnost informací – Information Security Management Systém (ISMS)

Aby bylo možné řídit organizaci dle norem, je třeba klást důraz na následující činnosti:

- pochopení požadavků, potřeb a očekávání zainteresovaných stran
- potřeba stanovení zásad a cílů
- zavedení systémových opatření
- monitorování a hodnocení funkčnosti a účinnosti systému řízení
- neustálé zlepšování založené na objektivních měřítkách účinnosti systému a tím dosažení udržitelného úspěchu organizace

Následující obrázek ukazuje vztah mezi komponenty IMS. (2)

Obrázek 2 Vztah mezi komponenty integrovaného systému řízení



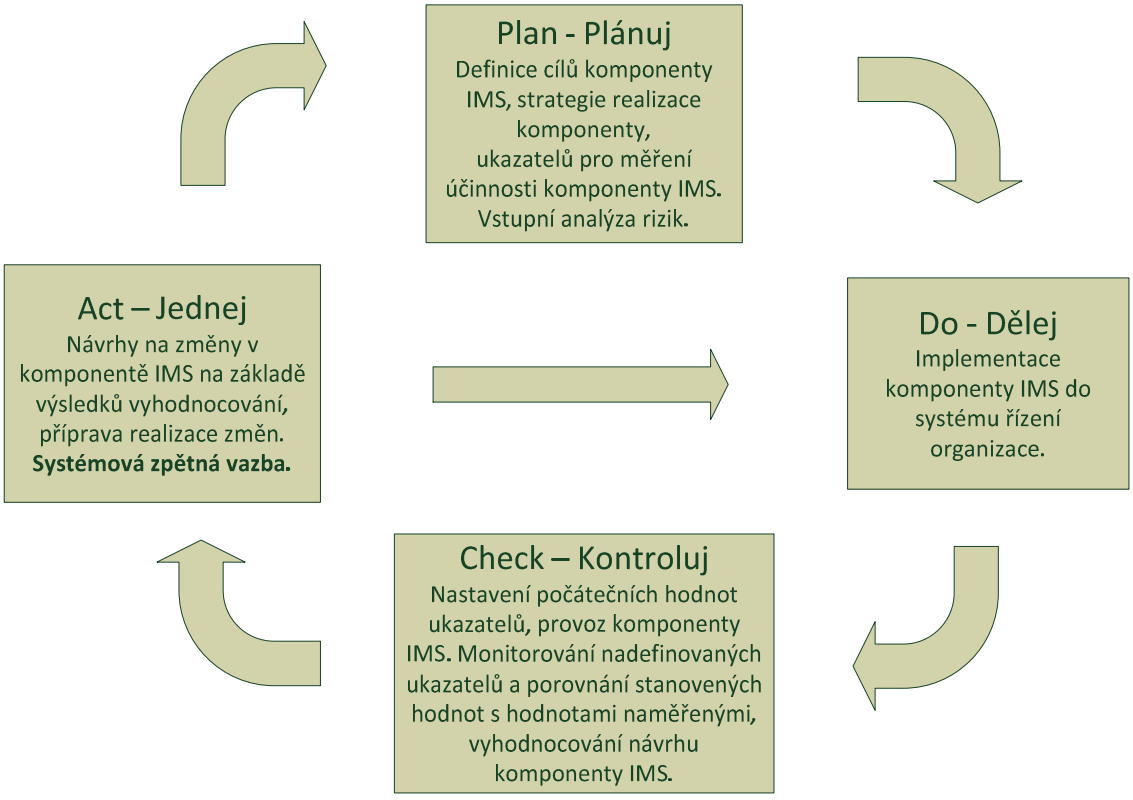
3.8 Model PDCA v IMS

Integrovaný systém řízení má jeden důležitý rys. Při řízení jeho komponent je možné použít obdobné postupy a metody. Tyto postupy lze zahrnout do životního cyklu vytváření a řízení každé z komponent IMS.

Tento životní cyklus vychází z manažersky ověřeného konceptu řízení PDCA. Tento koncept PDCA se označuje rovněž jako Demingův model. Původně byl navržen pro inovace a nasazování systému řízení v průmyslu. Nyní ho využívají normy v oblasti IMS i v oblasti řízení bezpečnosti informací.

Model PDCA se skládá ze 4 kroků. Jde o plánování – Plan, dělání – Do, kontrolu – Check a zlepšování – Act.

Obrázek 3 Demingův model PDCA a IMS



3.9 Analýza rizik a bezpečnostní politika

3.9.1 Analýza rizik

Při provádění ISMS je jedním z nejdůležitějších kroků vypracování analýzy rizik. Tento krok se uskuteční v počáteční fázi provádění ISMS. Analýza rizik je pro celé provedení ISMS klíčová. Aby mohla být analýza rizik sestavena, je doporučeno provést několik kroků, které jsou:

- Stanovení hranice analýzy rizik – na začátku je nutné určit, která aktiva se budou do vytvářené analýzy rizik začleňovat a která ne. Tím se stanoví výsledný rozsah analýzy. Určení hranice stanovuje vedení organizace na základě úvodní studie, nebo sledované oblasti aktiv.
- Identifikace aktiv – pod zvolenou hranicí se vytvoří soupis všech identifikovaných aktiv.
- Stanovení hodnoty a seskupování aktiv – hodnoty aktiv lze stanovit podle různých hledisek. Převážně to jsou hlediska nákladů nebo výnosů. Vždy se použijí ta, která mají pro podnik větší hodnotu. Charakteristikami pro stanovení hodnot můžou být např. pořizovací ceny, ochranné známky, patenty, zisky z aktiv, technologie, know-how atd. Do hodnot se započítává i to, jak je organizace na daném aktivu závislá, co se v organizaci stane v případě nedostupnosti, zničení, ztrátě nebo výpadku aktiva.

  V organizaci bývá většinou identifikováno mnoho aktiv, proto je dobré je shromažďovat do skupin. Tyto skupiny by měly mít aktiva podobné povahy a měla by se pro ně zavádět společná opatření.
- Identifikace hrozeb – v další části analýzy rizik jsou vyhledány hrozby, pro které v následujících krocích musí být zvoleno vhodné protiopatření. Tyto hrozby musí ohrožovat alespoň jedno z aktiv, které bylo vybráno v předchozím kroku. Hrozby lze identifikovat mnoha způsoby, např. z oborových zkušeností, z provedené analýzy, nebo z literatury. Pro každou organizaci jsou hrozby jiné, podle toho v jakém odvětví působí, proto se někdy využívá pro identifikaci i metod jako je brainstorming.
- Analýza hrozeb a zranitelnosti – všechny identifikované hrozby je nutné hodnotit se všemi skupinami aktiv, které jsme sestavily. U aktiv, na kterých se

může projevit některá hrozba, se stanovuje úroveň hrozby vůči aktivu a rovněž úroveň zranitelnosti aktiv k hrozbě. Pro stanovení úrovně hrozby se používají faktory jako nebezpečnost, motivace a přístup. Pro stanovení zranitelnosti se používá citlivost a kritičnost. Při analýze hrozeb se berou v potaz případná protiopatření, protože ta mohou snižovat úroveň hrozby i zranitelnosti.

- Pravděpodobnost jevu – u výskytů hrozeb se uvažuje i nad pravděpodobností výskytu daných hrozeb. Při analýze hrozeb je tedy nutné hrozby ještě doplnit o pravděpodobnost, s jakou nastanou a s těmito hodnotami počítat při vytváření odpovídajících protiopatření. U vyjádření pravděpodobnosti jevu se zkoumá, jestli jsou jevy náhodné, nebo ne a jestli jsou ve zvolené úrovni pravděpodobnosti.
- Měření rizika – riziko je měřeno pomocí předchozích kroků. Počítáme tedy s hodnotou aktiva a s úrovní hrozby a zranitelnosti aktiva. Protože jsou rizika převážně neměřitelná, je stanovení hodnoty rizika obtížné určit. Rizika jsou tedy většinou odhadována specialistou, který má s jejich stanovením praxi. Hodnotí se většinou slovním popisem, jako je riziko malé, střední nebo vysoké.

  Při měření se také počítá s pravděpodobností výskytu jevu, kdy větší pravděpodobnost znamená logicky větší míru rizika. (8)

3.9.2 Bezpečnostní politika

Při zavádění ISMS v organizace je jedním z hlavních kroků vytvoření bezpečnostní politiky. Bezpečnostní politika je dokument, který určuje interní směrnice, zavádí pravidla, definuje postupy řízení, ochrany a zacházení s informačními aktivy. Při vytváření bezpečnostní politiky je třeba, aby byla podporována vedením organizace.
Minimální obsah bezpečnostní politiky by měl mít:

- Odkazy na dokumentaci, ve které lze zjistit detailnější bezpečnostní politiku, postupy ve specifických oblastech nebo bezpečnostních pravidlech, které by měly osoby dodržovat.
- Záměr vedení organizace podporovat cíle a zásady bezpečnosti informací.
- Definice bezpečnosti informací, její rozsah, důležitost, cíle a význam.

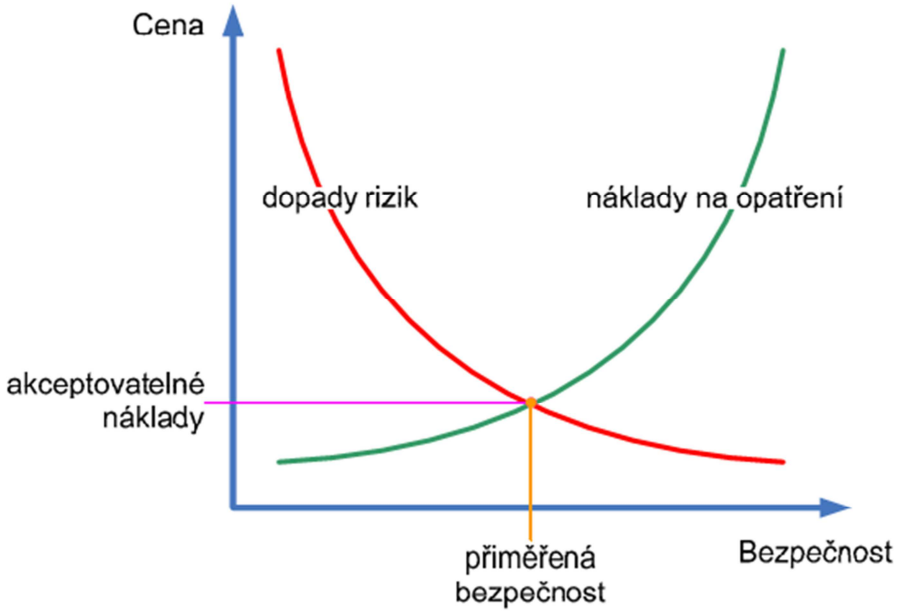
- Definice obecných a specifických zodpovědností pro řízení bezpečnosti informací a také pro hlášení případných bezpečnostních incidentů.
- Stručné objasnění bezpečnostních zásad, standardů, principů a případné speciální požadavky.

Je vhodné zpracovat až tři úrovně bezpečnostní politiky, tak jak to udávají kritéria hodnocení bezpečnosti informačních systémů – ITSEC:

- Celková bezpečnostní politika – ta stanovuje cíle a popis principu zajištění celkové bezpečnosti informačních systémů se vztahem k bezpečnosti organizace.
- Systémová bezpečnostní politika – ta udává, jak je možné zajistit bezpečnost informačního systému v organizaci. Řeší se v ní podrobněji popis vnitřních a vnějších vazeb IS organizace, popis bezpečnostních opatření informačních systémů, vyhodnocování analýzy rizik informačního systému a způsob ochrany aktiv informačního systému.
- Technická bezpečnostní politika – popisuje konkrétní opatření, která zajišťují bezpečnost při zpracování informací a při využívání zdrojů v organizaci.

Při zavedení ISMS je nutné v pravidelných intervalech, např. jednou ročně přezkoumat bezpečnostní politiku. Cílem přezkoumání je zajištění, aby bezpečnostní politika byla v souladu se skutečností a aby byla posouzena adekvátnost a efektivnost navržených a používaných opatření. Případně se na základě přezkoumání provedou úpravy, které by měly odpovídat aktuálním potřebám organizace.

Obrázek 4 Přiměřená bezpečnost



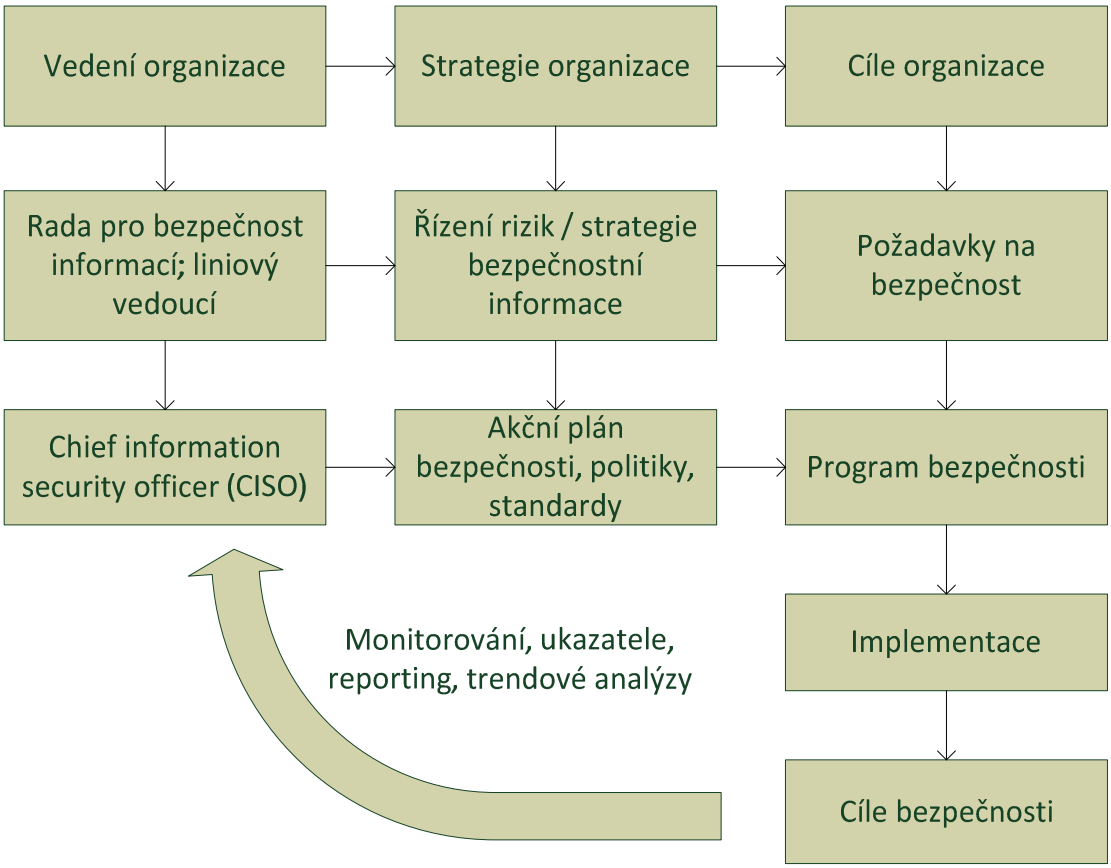
Zdroj: Prezentace z předmětu Management informační bezpečnosti (9)

3.10 ISMS - Management bezpečnosti informačních systémů

Management bezpečnosti informačních systémů je soubor pravidel a opatření, která umožňují osobě poskytnout správné a úplné informace ve správnou dobu a to pouze té osobě, která je k jejich získání oprávněná. Zajišťují se tak principy integrity, dostupnosti a důvěrnosti.

Zavedení managementu bezpečnosti informačních systémů není jednoduché. Jak již bylo zmíněno, neexistuje na to žádné univerzální řešení. Každá organizace má jiné potřeby, jinou strukturu, jiné zaměření atd. Jedná se také o dlouhodobý proces, který díky tomu, že se využívá model PDCA nemá dohledný konec. Je to ovšem logické, protože se postupem času mění i možná rizika a hrozby, na ty je nutné reagovat, a tak zdokonalovat systém v organizaci.

Obrázek 5 Model řízení informační bezpečnosti v organizaci



Zdroj: Vlastní zpracování (8)

3.11 Základní požadavky ISMS

Pro implementaci ISMS v organizaci existují následující kroky:

- Ustanovení
- Zavádění
- Provoz
- Monitorování
- Přezkoumávání
- Udržování
- Zlepšování

Všechny kroky musí být důkladně zdokumentovány. Proces zavedení ISMS v organizaci, který je popsán v ČSN ISO/EN 27001:2006 vychází z modelu PDCA.

V tomto modelu jsou shromážděny předchozí kroky do 4 základních procesů:

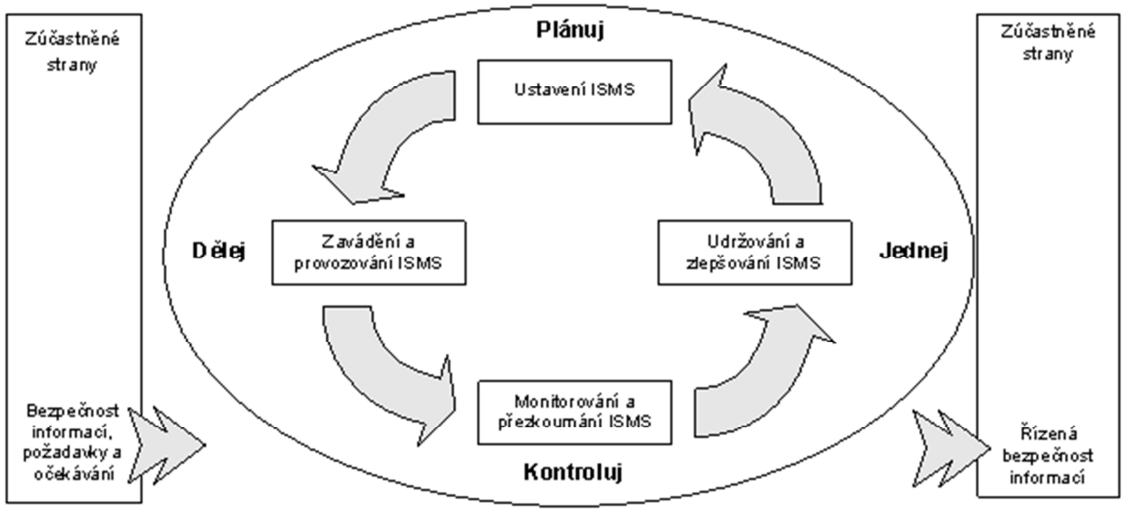
1. První proces **Plánuj** obsahuje krok ustanovení ISMS. Ten obnáší definici cílů, postupů a procesů a vytvoření politiky ISMS. Definované cíle, postupy a procesy musí odpovídat řízení rizik tak, aby se splnily cíle organizace a cíle vytvořené v politice ISMS.
2. Druhý proces **Dělej** obsahuje krok zavádění a provoz ISMS. Jedná se o uskutečnění vytvořené podnikové politiky, realizaci postupů a procesů tak, aby byly splněny zvolené cíle.
3. Třetí proces **Kontroluj** obsahuje kroky monitorování a přezkoumávání ISMS. V tomto procesu se posuzují provedené výkony s politikou ISMS, s definovanými cíli a s praktickými zkušenostmi. Podává se v pravidelných intervalech hlášení o výsledcích vedení organizace, které může přezkoumat dosavadní postup ISMS.
4. Čtvrtý proces **Jednej** obsahuje kroky udržování a zlepšování ISMS. Jsou zde přijata opatření, která napravují zjištěné problémy. Rovněž se zde vytváří preventivní opatření, jejichž podnět vzniku byl dán interním auditem ISMS. Neustálou kontrolou a následným vznikem opatření dochází k zlepšování ISMS.

Při zavádění ISMS jsou jednotlivé procesy navrhovány tak, aby byla zaručena přiměřená a efektivní opatření, která mají za úkol chránit stanovená aktiva organizace.

Tato opatření musí být navržena tak, aby vyhovovala i dalším zúčastněným stranám a zároveň byla finančně únosná.

Na následujícím obrázku, je uveden model PDCA aplikovaný na procesy ISMS.

Obrázek 6 Demingův model PDCA implementovaný na jednotlivé procesy ISMS

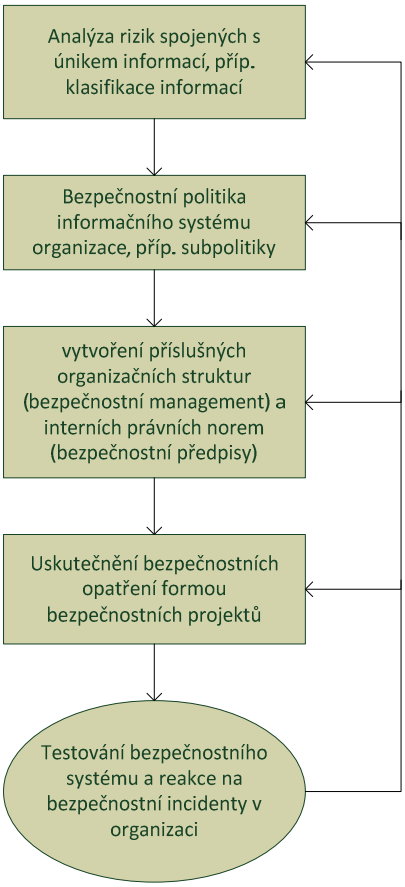


Zdroj: ČSN ISO/IEC 27001:2006 (7)

3.12 Proces zavádění ISMS

Zavádění ISMS lze popsat následujícím obrázkem.

Obrázek 7 Vytvoření informační bezpečnosti opakovaným procesem



Zdroj: Vlastní zpracování (8)

3.12.1 Ustanovení ISMS

Podle ČSN ISO/IEC 27001 je nutné splnit v rámci ustanovení ISMS tyto požadavky:

- V první řadě jde o zanalyzování organice. To obsahuje určení činností organizace, její umístění, používaná aktiva a technologie a vnitřní uspořádání. Na základě analýzy se stanoví rozsah a hranice zaváděného ISMS. Pokud jsou některé aspekty organizace vyjmuty z procesu ISMS musí se zaznamenat důvody tohoto počínání.
- Ze znalostí rozsahu zaváděného ISMS je následně nutné stanovit politiku ISMS v organizaci. Tato politika zahrnuje požadavky plynoucí z činnosti organizace a ze zákonů v zemi, dále cíle a směr řízení činností v okruhu bezpečnosti informací.

- Další bod se týká rizik. Je nutné stanovit, jak budou rizika hodnocena a jaká budou měřítka pro akceptaci rizika. Vybraný postup hodnocení rizik musí zajišťovat možnost porovnání a opakování zjištěných výsledků.
- Dále je nutné stanovit aktiva a jejich vlastníky, najít pro ně možné hrozby a najít zranitelná místa. Stanovit, jaký vliv by měla na aktiva ztráta integrity, dostupnosti a důvěrnosti.
- V dalším kroku je provedena analýza a vyhodnocení rizik. Je zde řešena otázka, co by se stalo, kdyby došlo k bezpečnostnímu incidentu, kdyby byla ztracena integrita, dostupnost a důvěrnost, jestli je možnost selhání bezpečnosti a jak velké by byly následky. Určí se akceptovatelná velikost rizika, podle které se na jednotlivá rizika vytvoří opatření, nebo se pouze vezmou v potaz.
- Dále se popisuje aplikace opatření na zvolená rizika, která nelze přesunout na třetí stranu nebo je nelze pouze akceptovat.
- Poté jsou určeny cíle jednotlivých opatření, kde se musí stanovená opatření zdůvodnit podle hodnocení a zvládání rizik.
- Ostatní rizika se odsouhlasí vedením organizace.
- Vedení dá rovněž povolení k zavedení a provozu ISMS.
- Poslední požadavkem je sepsání Prohlášení o aplikovatelnosti. To sumarizuje předchozí kroky a jsou v něm zapsány cíle, vybraná opatření společně se stanovenými důvody, aplikovaná opatření použité v podniku a vyloučená rizika s důvody, proč byla vyloučena.

3.12.2 Zavádění a provozování ISMS

V části zavádění a provozování ISMS jsou kroky organizace dle normy ČSN ISO/IEC 27001 následující:

- Je vytvořen plán pro zvládání rizik, který popisuje konkrétní činnosti pro vedení, zdroje a stanovuje prioritní činnosti při řízení rizik v bezpečnosti informací.
- Je zaveden plán na zvládání rizik do organizace. A to tak, aby se dosáhlo cílů stanovených opatření. Jsou přiřazeny role a odpovědnosti osobám s ohledem na finanční zdroje.

- V tomto kroku je již aplikováno vybrané bezpečnostní opatření tak, aby bylo dosaženo stanoveného cíle tohoto opatření.
- Jsou stanoveny metriky, díky kterým se budou aplikovaná opatření sledovat a vyhodnocovat jejich účinnost. Tyto metriky jsou stanoveny tak, aby bylo možno sledování a vyhodnocování opakovat a výsledky bylo možné porovnávat.
- Další krok je řízení zdrojů a provozu ISMS.
- Posledním krokem v zavádění a provozování ISMS je implementace postupů a opatření, které mají rychle detekovat a reagovat na bezpečnostní incidenty.

3.12.3 Monitorování a přezkoumání ISMS

Monitorování a přezkoumání ISMS má opět několik kroků:

- Provádí se zde monitorování, kontrolování a v případě nutnosti se zavádí nová opatření pro detekci chyb při zpracování, pro identifikaci pokusů o narušení, ať už úspěšných či nikoli. Vedení organizace by mělo být schopno posoudit, jestli pověřené osoby a použité technologie dobře plní svoji roli. Dále se vyhodnocuje, jestli jsou opatření proti narušení spolehlivá.
- Pravidelně se provádí také přezkoumání účinnosti ISMS, která jsou zaměřena na splnění politiky, cílů a opatření. V potaz se berou i výsledky incidentů, auditů a měření účinnosti opatření. K tomu je ještě nutné sledovat připomínky a návrhy zúčastněných stran.
- Dalším krokem je ze získaných výsledků měření implementovaných opatření zjistit, jestli jsou splněny požadavky bezpečnosti.
- V pravidelných intervalech se přezkoumávají rizika. Zkoumá se, jestli nevznikají nová rizika, nebo se nezmění váha akceptovaných rizik vzhledem ke změně v organizaci, nebo nové vzniklé hrozbě.
- V pravidelných intervalech se také provádí vnitřní audity.
- Vedení organizace provádí přezkoumání ISMS, aby byl zajištěn ideální rozsah opatření a mohlo být případně ISMS v organizaci zlepšeno.
- Přezkoumáváním a monitorováním je nutné k aktualizování bezpečnostních plánů.
- Účinnost opatření a činnosti i události s dopadem na ISMS je třeba všechny pečlivě zaznamenávat.

3.12.4 Udržování a zlepšování ISMS

Aby se ISMS stále zlepšovalo a udržovalo, je nutné pravidelně zavádět nové identifikované zlepšení ISMS, provádět nápravná a preventivní opatření s ohledem na naše získané zkušenosti i zkušenosti jiných subjektů, kteří se pohybují v oblasti bezpečnosti. Zavádění nových návrhů a činností je nutné konzultovat se zainteresovanými stranami a řídit postup jejich zavádění. Součástí procesu zlepšování je i kontrola, zda daná zlepšení splnila stanovené cíle.

3.13 Požadavky na dokumentaci

Každé rozhodnutí, které je učiněno vedením organizace a každá činnost musí být zpětně dohledatelná v záznamech. Aby byla zajištěna opakovatelnost, musí být záznamy kvalitně dokumentovány. Zaznamenávají se rovněž vztahy mezi výsledky z hodnocení procesu a riziky, vazbou na politiku ISMS a vybranými opatřeními. Rozsah dokumentace ISMS se odvíjí od velikosti organizace a její činnosti a bere se v potaz i složitost systému.

V dokumentaci ISMS jsou zahrnuty:

- opatření a postupy podporující ISMS
- zprávy o hodnocení rizik
- metodiky hodnocení rizik
- cíle, politika a rozsah ISMS
- plány, které popisují způsob zvládání rizik
- prohlášení o aplikovatelnosti
- záznamy o výskytech bezpečnostních konfliktů a výkonu procesu
- nezbytné postupy nutné k zajištění provozu a řízení procesů ISMS, efektivnímu plánování a k měření účinnosti různých opatření

3.13.1 Řízení dokumentů

Dokumenty, které jsou vytvořeny v souvislosti s ISMS by měly být řízeny a chráněny. Měl by být vypracován dokumentový postup, který slouží pro řídící činnost, která je nutná pro:

- schválení dokumentu před tím, než je vydaný
- případnou aktualizaci dokumentů a jejímu dalšímu schválení
- identifikaci změn dokumentů a současného stavu přezkoumání dokumentů
- čitelnost a jednoduchou identifikaci dokumentů
- dostupnost pravidel, která popisuje, jak manipulovat s těmito dokumenty
- přesné stanovení původu dokumentu, hlavně když je z externího prostředí
- řízení šíření dokumentů, tak aby bylo zabráněno používání starých dokumentů

3.14 Odpovědnost vedení

Vedení organizace musí podporovat veškeré činnosti, které jsou zavedení, provoz, monitorování, přezkoumávání a zlepšování ISMS. Podporu těchto činností by mělo být vedení schopno doložit. V politice, stanovených cílech a plánech ISMS je podpora vedení přímo vyjádřena.

Vedení má také odpovědnost za nastavené povinnosti, odpovědnosti a role v řešení ISMS.

Aby zavedené ISMS plnilo stanovené cíle, bylo v souladu s bezpečnostní politikou, byla nastavena odpovědnost plynoucí ze zákona a bylo soustavně zlepšováno, je nutné všechny činnosti dostatečně v organizaci propagovat.

Vedení organizace nastavuje hranici pro akceptování rizika, stanovuje přijatelnou velikost zůstatkového rizika a v neposlední řadě je jeho povinností, aby sehnalo dostatečné (nejen finanční) zdroje pro celý proces ISMS a vykonávání interních auditů.

3.15 Audity

Interní audity ISMS se v podniku musí provádět v naplánovaných intervalech. Audity posuzují, jestli vyhovují cíle, bezpečnostní opatření, postupy a procesy ISMS požadavkům, které udává zákon, norma ČSN ISO/IEC 27001:2006 a regulatorní

požadavky. Dále se kontroluje, jestli postupy ISMS souhlasí s nastavenými požadavky na bezpečnost, jestli jsou zavedeny, prováděny a efektivně udržovány.
Interní audity se provádějí s ohledem na stav, v jakém jsou auditované procesy. V potaz se berou stavy procesů v předchozích auditech. Při prováděných interních auditech jsou stanoveny kritéria, počet opakování, rozsah a použité metody. Auditoři musí být nestranní a objektivní. Proto nesmí auditovat svoji vlastní práci. I u auditů se musí požadavky, odpovědnosti, hlášené výsledky a nakládání s audity dokumentovat.
Po provedeném auditu a zjištění nedostatků musí vedení organizace bezodkladně zajistit odstranění těchto nedostatků. Kroky na nápravu musí být zkontrolovány a rovněž zdokumentovány.

3.16 Řízení zdrojů

3.16.1 Zabezpečení zdrojů

Aby bylo možné provozovat ISMS v organizaci, je proto nutné zajistit odpovídající zdroje. Ve shodě s politikou bezpečnosti a s prohlášením o bezpečnosti zajišťuje zdroje vedení organizace. Tyto zdroje jsou využity pro ustavení, zavedení, provoz, monitorování, udržování a zlepšování ISMS organizace.

3.16.2 Odborná způsobilost zaměstnanců

Odborná způsobilost zaměstnanců je nutná u všech úkolů, které jsou v rámci ISMS prováděny. Proto je nezbytné provádět patřičná školení, nebo zaměstnat již způsobilé zaměstnance. Provedená školení se zpětně vyhodnocují a u zaměstnanců se vedou záznamy o absolvovaných školeních, o jejich vzdělání, zkušenostech a dovednostech. Samozřejmě je nutné zaměstnance poučit o důležitosti prováděných činností a také o jejich podílu na dosahování cílů ISMS.

3.17 Přezkoumání ISMS

ISMS se v organizaci musí přezkoumávat v pravidelných intervalech. Maximální délka intervalu je jeden rok. Díky tomuto přezkoumání se navrhují změny a zlepšení pro ISMS včetně změn bezpečnostní politiky a cílů. Po provedeném přezkoumání se

všechny fakta, návrhy, zlepšení, a uskutečněné události musí zaznamenat dle platných pravidel dokumentování.

3.17.1 Podklady pro přezkoumání

Do přezkoumávání ISMS se zahrnují tyto podklady:

- podklady od zainteresovaných stran v rámci ISMS
- zjištěné výsledky minulých přezkoumávání ISMS a výsledky auditů
- informace o možném zlepšení účinnosti ISMS
- podklady o preventivních opatřeních
- informace o možných hrozbách, které nejsou zapracovány do ISMS
- informace o měření účinnosti zavedených opatření
- postup, který byl proveden po předchozím přezkoumání
- informace o změnách, které ovlivňují bezpečnost informací

3.17.2 Výsledky z přezkoumání

Výsledky z přezkoumání jsou určité činnosti a rozhodnutí, které souvisí s:

- zlepšením účinnosti ISMS
- změnami v hodnocení rizik nebo s plánem k jejich zvládnutí
- potřebou dalších zdrojů
- postupy, které by měly umožnit lepší měření účinnosti opatření
- změnami v postupech v bezpečnosti informací, v návaznosti na vnější nebo vnitřní události, které mají vliv na ISMS

3.18 Zlepšování ISMS

Po zavedení systému ISMS do organizace nastává nekončící koloběh. Denně vznikají nová rizika, na která je nutné reagovat. Kvůli tomu se proces ISMS musí neustále zlepšovat, zlepšuje se bezpečnost informací, analýza monitorovaných událostí, nápravná a preventivní opatření.

Opatření lze rozdělit do dvou skupin. Jedna z nich jsou nápravná opatření a druhá preventivní opatření.

3.18.1 Nápravná opatření

Nápravná opatření v provozovaném systému ISMS umožňují vyloučit opětovný výskyt vzniklých nedostatků. Nápravná opatření jsou zdokumentována a měla by být schopná předat informace o:

- zjištění nesouladu v provozu ISMS
- důvodu příčin nesouladu
- zhodnocení opatření, jestli zajišťují, aby opakovaně nevznikly problémy
- zavedených opatřeních, která slouží k nápravě problémů
- výsledcích z přijatých opatření
- opětovných přezkoumáních u zavedených opatření

3.18.2 Preventivní opatření

Preventivní opatření bývají většinou méně finančně náročná, než opatření nápravná. V organizaci v rámci ISMS by se měla definovat preventivní opatření, která by měla odpovídat závažnosti rizik, na která jsou tato opatření zaměřena. Organizace musí stále vyhledávat nová rizika nebo změny ve stávajících rizicích a zajišťovat preventivní opatření na významná rizika.

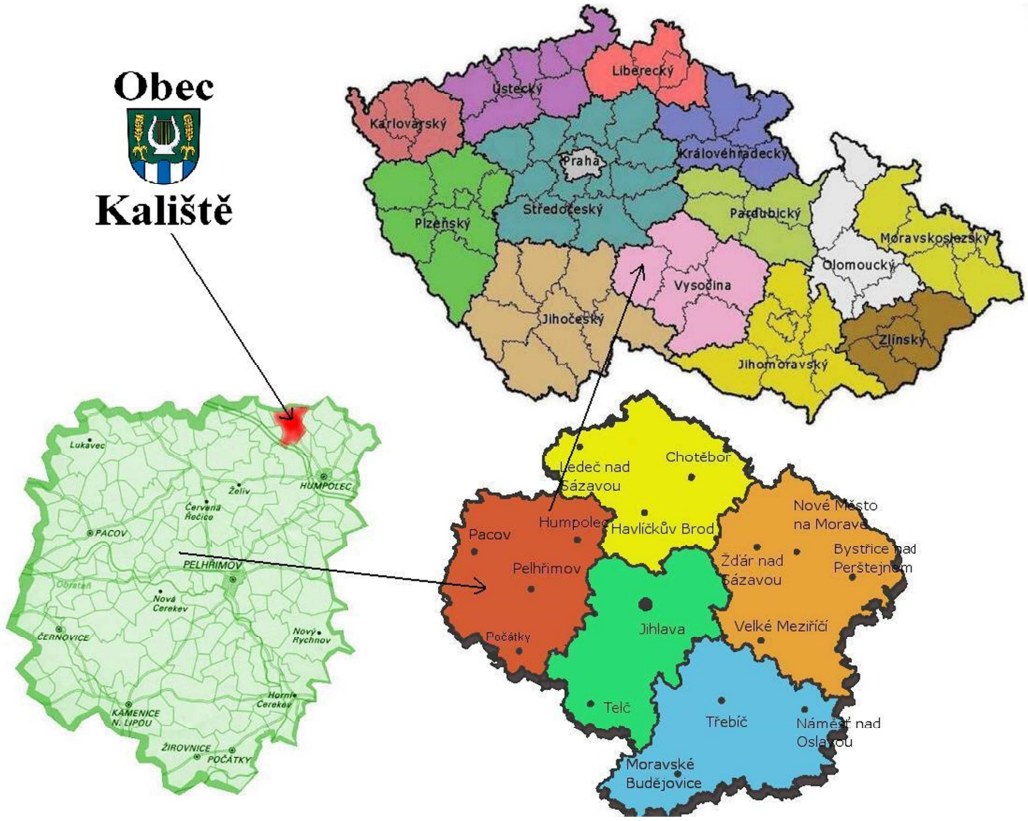
4 Analýza problému a současné situace

Aby bylo možné dobře rozpoznat problémy, které by se mohly nacházet v analyzované organizaci, je nutné tuto organizaci nejprve popsat.

4.1 Popis obce

Touto prací analyzovaná organizace je obecní úřad, který se nachází v Obci Kaliště. Tato obec je obcí I. typu. K 1. lednu 2013 měla obec 342 obyvatel, kteří žijí většinou v rodinných domech. Obec Kaliště leží v kraji Vysočina v bývalém okrese Pelhřimov, jak je znázorněno na obrázku. Pod obec spádově patří další 3 vesnice a to: Podivice, Holušice a Háj.

Obrázek 8 Poloha obce Kaliště

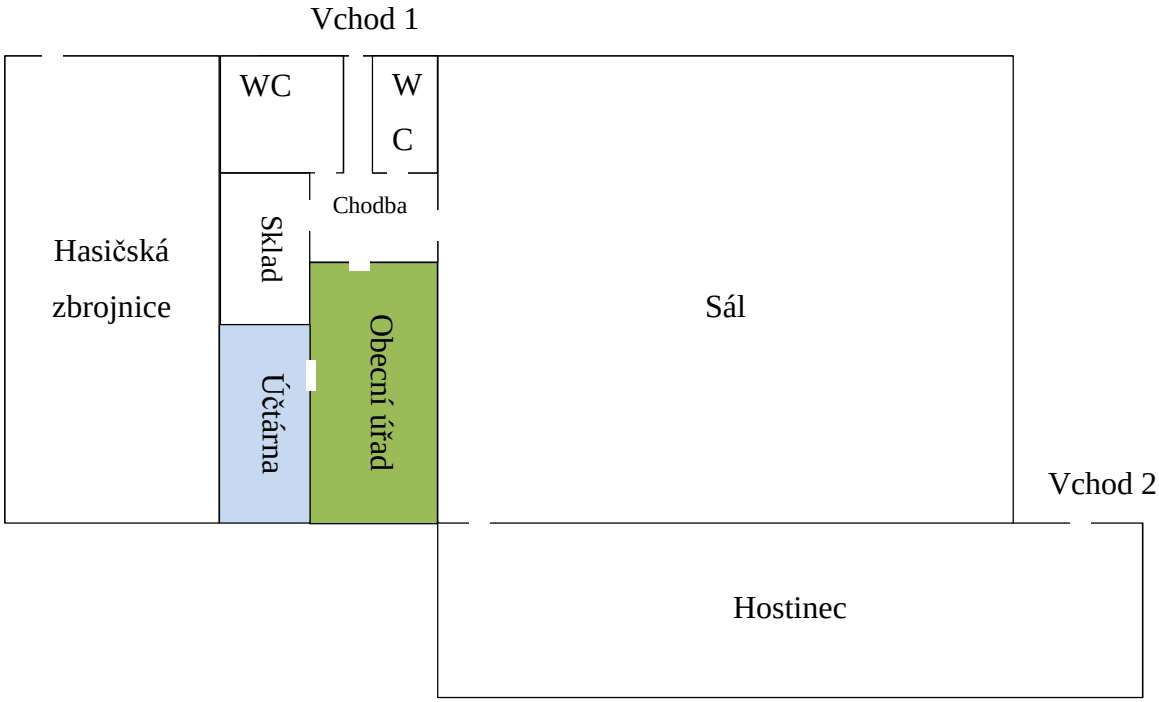


Zdroj: vlastní zpracování

4.2 Poloha obecního úřadu a popis rozmístění místností

Obecní úřad je umístěn přibližně uprostřed obce. Nachází se v budově, která je víceúčelová. V budově se nachází rovněž hasičská zbrojnice a slouží rovněž jako jeden z místních hostinců a je zde umístěn také největší sál, který se v obci využívá. Sociální zařízení je společné jak pro hostinec, tak pro obecní úřad. Kolem obecního úřadu se proto pohybuje velké množství osob.

Obrázek 9 Rozmístění místností v budově



Zdroj: Vlastní zpracování

Z následujícího nákresu je patrné, že do obecního úřadu se dá vstoupit jak přes vchod 1, tak přes vchod 2. Během provozní doby obecního úřadu je otevřen pro občany vchod 1. V nočních hodinách při provozu hostince je otevřen vchod 2. V tuto dobu již bývá obecní úřad uzamčen a návštěvníci hostince využívají sociální zařízení, které je umístěno u obecního úřadu. Kolem vstupu do obecního úřadu tak prochází mnoho lidí. Do účtárny lze projít pouze přes obecní úřad a bývá vždy ještě speciálně uzamčena. Vchod do hasičské zbrojnice je oddělen, ale jen z hasičské zbrojnice je možný vstup na půdu, která je nad celým objektem.

4.2.1 Obecní úřad - kancelář starosty obce

Místnost obecního úřadu je také kanceláří starosty obce. Jsou zde prováděna jednání zastupitelstva a občané na toto místo chodí v rámci řešení různých problémů. Přístup do této místnosti má i hajný obecních lesů a místostarosta, kteří mají vlastní přístupová hesla a klíče. Ostatní občané obce mají volný přístup do této místnosti v době úředních hodin.

4.2.2 Účtárna

V účtárně pracuje jedna účetní, která má na starost veškeré účetnictví obce. Účtárna slouží také jako podatelna. Za účetní rovněž chodí občané obce převážně v dobu, kdy se platí různé poplatky obci a zde finanční prostředky předávají. Účtárna tedy slouží i jako pokladna pro obecní úřad. Občané obce do účtárny mají volný přístup rovněž, když jsou úřední hodiny obecního úřadu.

4.2.3 Personální situace

V rámci obecního úřadu pracuje tedy starosta a účetní. Každý pátek přichází na konzultaci změn místostarosta obce. Do místností obecního úřadu má vlastní přístup i hajný obecních lesů.

Zaměstnanci obecního úřadu neabsolvují žádná bezpečnostní školení. Pouze účetní jednou ročně absolvuje školení o změnách v účetnictví. Neprovádí se tedy ani žádná školení v rámci prací s výpočetní technikou, která by usnadnila práci zaměstnancům.

4.2.4 Struktura informačních technologií

Interní síť organizace je vytvořena svépomocí, nebyla najata žádná firma, která by měla na starost vytvoření a chod sítě. Funkčnost sítě je velmi omezená. Prostředky na chod informačních technologií jdou z obecního rozpočtu a prostředky na inovaci nebo nákup nových zařízení jsou čerpány z dotací, které jsou během let vypisovány. Poslední dotace na zajištění technologií byla v rámci projektu Czech Point.

Přístup na internet je sjednán se společností O2, která má na budově umístěn převaděč wifi signálu a po domluvě neplatí nájem za umístění, ale poskytuje internet obecnímu úřadu. Nicméně rychlost tohoto internetu je velmi nízká 2/1 Mbit.
V místnosti obecního úřadu je umístěn 4 portový switch, do kterého je zapojen kabel, který rozděluje datový proud do stolního počítače umístěného v kanceláři obecního úřadu a do stolního počítače umístěného v účtárně. Poslední port je využíván pro notebook, který obecní úřad také vlastní. Wifi síť není na obecním úřadě vytvořena, i když by to některé zahraniční návštěvy velmi uvítaly.[4] Kabeláž je umístěna pouze v nezabezpečených kabelových žlabech.
Na obecním úřadě nejsou použity žádné záložní zdroje, pouze u stolního počítače na obecním úřadě je zajištěna přepěťová ochrana.

V místnosti obecního úřadu je umístěn stolní počítač, na kterém je umístěna většina dat, která jsou nutná pro chod obecního úřadu. Data nejsou nikterak zálohována ani šifrována. Na tomto počítači je nainstalován operační systém Windows Vista. Kancelář je dále vybavena jednou barevnou laserovou tiskárnou, která je připojena prostřednictvím usb kabelu ke stolnímu počítači a dále je zde jedna multifunční rovněž barevná tiskárna.

V účtárně je umístěn starší počítač se systémem Windows XP, na kterém je nainstalován především účetní program Triada a další software nutný pro výkon administrativní činnosti. K tomuto počítači je rovněž připojena prostřednictvím usb kabelu černobílá laserová tiskárna.

Obecní úřad provozuje vlastní webové stránky, které byly vytvořeny externí firmou a jsou spravovány pověřenou osobou v obci. Obec má zřízenu jednu veřejnou emailovou adresu: kaliste@quick.cz. Tato emailová schránka má kapacitu pouze 10 MB.
Mezi jednotlivými počítači bylo svépomocí vytvořeno několik sdílených složek, především na sdílení dokumentů mezi účetní a starostou. Mezi stolním počítačem na

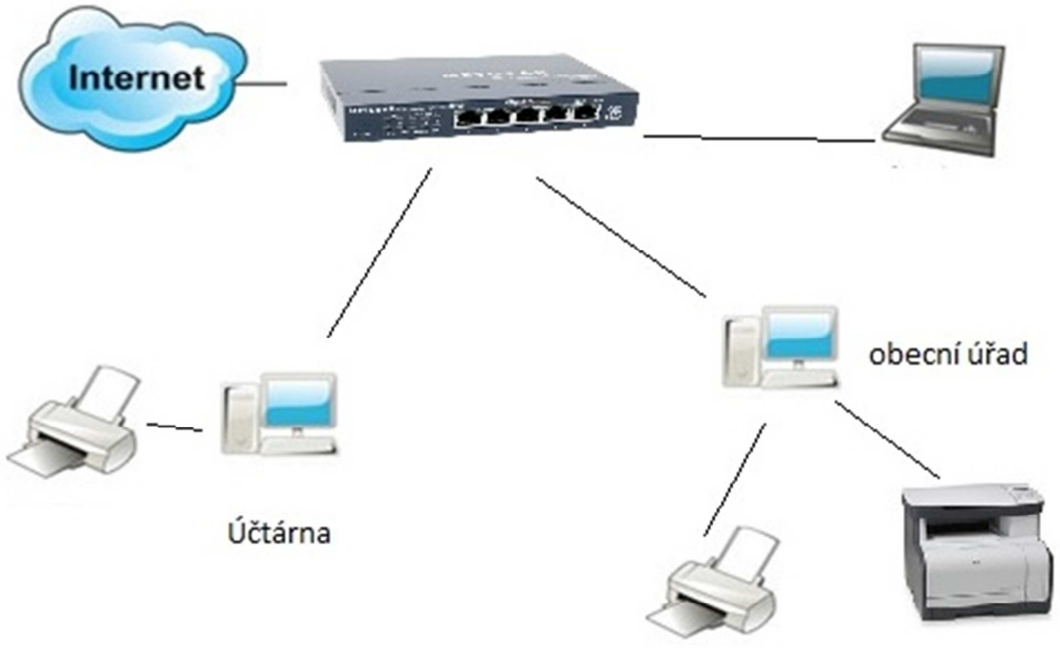
[4] Do obce přijíždí každoročně velké množství zahraničních turistů. Jedná se především o Němce, Rakušany a Japonce. Důvodem jejich návštěv je zesnulý významný hudební skladatel a dirigent Gustav Mahler, který má v obci Kaliště rodný dům.

obecním úřadu a notebookem je vytvořeno rovněž sdílení některých dokumentů pomocí cloudového úložiště.

Softwarová bezpečnost je zajištěna integrovaným firewallem a antivirem od firmy Eset. Na notebooku a stolním počítači v účtárně je vytvořen pouze jeden administrátorský účet, který není zabezpečen heslem.
Na stolním počítači starosty obce jsou vytvořeny čtyři uživatelské účty, jeden pro starostu obce, jeden pro místostarostu, jeden pro hajného a jeden pro ostatní uživatele.

Stolní počítač na obecním úřadě a notebook se používají pro přístup k systému Czech POINT a k datové schránce obce. K tomuto účelu má zřízen starosta i účetní certifikát s roční platností umístěný na usb tokenu.

Obrázek 10 Komponenty infrastruktury obecního úřadu



Zdroj: Vlastní zpracování

4.3 Poloha a zabezpečení objektu

Obec Kaliště leží v nadmořské výšce 602 m. n. m. a oproti okolním vesnicím leží na vyšším místě. Díky tomuto stavu v obci nehrozí žádné záplavy.

Jelikož je obec spádově rozložena a obecní úřad je uprostřed vsi, nehrozí zde úder blesku a od něj vznik požáru.

Ohrožení objektu je možné hlavně lidskou činností. Především z důvodu místního hostince a společných sociálních zařízení a také tím, že se zde koná mnoho zábav, kde se rovněž pohybuje spousta lidí.

Celý objekt je zabezpečen systémem od firmy BSBV. Je rozdělen na vchodové dveře a na odblokování různých místností. Např. pokud je otevřený hostinec, je odkódován pouze hostinec, sál, sociální zařízení a chodba. Při vstupu do jakékoli jiné místnosti se spustí alarm, stejně tak při použití 1. vchodu, který je odkódován pouze s obecním úřadem. Při odkódování obecního úřadu se naopak odkódují místnosti, které jsou nutné pouze pro činnost obecního úřadu.

Každá osoba využívající obecní úřad má vlastní přístupové kódy, podle kterých se pozná, kdo a kdy byl na obecním úřadě.

4.4 Řešení bezpečnosti v obci

Obecní úřad Kaliště patří k těm menším obecním úřadům, které lze v České republice nalézt. Vzhledem k tomu, že jsou v organizaci pouze 2 stálí zaměstnanci a každý týden komunikují s hajným, místostarostou a zastupiteli a všichni jsou občany jedné vesnice (kromě hajného, který je občan vedlejší vesnice), tak se velmi dobře znají a jsou mezi nimi neformální vztahy a i dobrá vzájemná důvěra. Tato situace nevede k tomu, aby se musela bezpečnost na obecním úřadě nějak vyžadovat. Odpovídá tomu i současný stav bezpečnosti v obci.

4.4.1 Bezpečnost fyzická

Fyzická bezpečnost je rozdílně zabezpečená ve vnějších a vnitřních prostorách.

Vnější prostory

Vnější prostory můžeme rozdělit na oblast mimo obecní úřad a oblast úplně mimo budovu. Vnější prostory mimo obecní úřad jsou celkově zabezpečeny proti

neoprávněnému vniknutí cizích osob. Zabezpečení je realizováno specializovanou firmou BSBV. Je omezeno v případě, kdy je otevřen hostinec. Toto zabezpečení klesá a je zabezpečen pouze obecní úřad a účtárna a vchod číslo 1. V ostatních částech budovy je umožněn pohyb osob. Dveře obecního úřadu oddělující chodbu jsou bezpečnostní, se skleněnými průhledy. Tyto dveře nahradily před měsícem starší obyčejné dveře s jedním velkým průhledem. Zvýšila se tak bezpečnost obecního úřadu. Okna budovy nejsou nijak zabezpečena, kromě oken obecního úřadu a účtárny. Ty jsou vybaveny mřížemi.
Vnější prostory mimo budovu nejsou nijak zabezpečeny.

Vnitřní prostory

Vnitřní prostor obecního úřadu není kromě zmíněného zabezpečení nijak chráněn. Při narušení bezpečnosti se spustí alarm a automaticky se volá starostovi obce na mobil a následně je tato událost nahlášena policii.
Po odkódování bezpečnostního systému je umožněn přístup všech osob, které přichází na obecní úřad v úředních hodinách, aby vyřídili vše potřebné.

4.4.2 Bezpečnost softwarová

Softwarová bezpečnost je řešena u každého počítače podobně. Každý počítač má firewall od Microsoftu. Notebook a stolní počítač na obecním úřadě je vybaven lepším firewallem od systémů Windows Vista a účtárna firewallem od Windows XP.
Každoročně je kupována licence na antivirový program NOD32 od společnosti ESET. Tento antivirový program je využíván na všech zmíněných počítačích.
Veškerá data nejsou nijak šifrována.

4.4.3 Vyhodnocení stávajícího stavu

Z předchozího popisu bezpečnosti vyplývá, že v obci není bezpečnost téměř vůbec řešena. Nejsou nijak zvlášť zabezpečena žádná data, natož ta citlivá, která by se chránit určitě měla. V obci nejsou stanoveny ani metodiky pro řešení bezpečnostních incidentů. Pracovní stanice nejsou chráněny proti výpadku proudu a je možné, že se neuložená data nenávratně ztratí. Přepěťová ochrana je aplikována pouze na stolním počítači

umístněném v obecním úřadě. Na zařízeních není prováděna žádná kontrola a může tak hrozit riziko ohrožení zdraví i majetku. Zavedení ISMS do obce by bylo velmi vhodné, vyřešily by se tak některé závažné nedostatky a snížilo riziko ztráty důležitých a chráněných dat.

V obci a na obecním úřadě má za většinu aktiv odpovědnost starosta obce. Účetní nese odpovědnost pouze za pokladnu a za dobře provedené účetnictví. Na hospodaření obce a na účetnictví je ze zákona prováděn audit.

Používáním slabých hesel a všemožnými zjednodušeními, jako je ukládání hesel a převážně neznalostí bezpečnostních rizik, které se vyskytují v okolí obce, je velmi pravděpodobné, že se do počítačů v obci dostane škodlivý kód. Tento kód, ať již špionážní, nebo poškozující by byl velkým problémem. Již dříve se stalo, že používáním velmi slabého hesla k veřejnému emailovému účtu obce došlo k napadení a zneužití tohoto emailového účtu k rozesílání spamu. Emailová schránka byla poté zablokována a nebylo možné se dostat k důležitým emailům, které jsou obci touto cestou zasílány.

Navazující kapitola této diplomové práce bude zaměřena na analýzu rizik a návrhů na řešení, která by snížila tato rizika. Po konzultaci se starostou obce se neuvažuje o certifikaci ISMS, ale je domluveno, že se bude postupovat podle normy ISO 27000, kdyby se v budoucnu změnil názor na certifikaci.

V obci se neprovádí žádná dokumentace procesů. Procesy jsou převážně známy jen osobě, která je provádí. V případě nemoci se proces neprovádí a čeká se, až se osoba vrátí do práce.

5 Vlastní návrhy řešení, přínos návrhů řešení

Před vlastním zavedením ISMS do obce je ještě nutno vyřešit několik otázek, týkajících se ustanovení ISMS.

5.1 Ustanovení ISMS

Ustavení ISMS definuje klíčové prvky, které mají vliv na realizaci ISMS. Je zde uveden rozsah ISMS, politika ISMS, plán zvládání rizik a metodika hodnocení rizik.

5.1.1 Rozsah ISMS

I když obec prozatím neplánuje certifikaci ISMS je i přesto zvolen postup podle normy ISO 27000, kdyby se v budoucnu obec rozhodla tento názor změnit. Rozsah ISMS bude použit na celou obec a nebude použit pouze na některou oblast. Z toho důvodu, že je obecní úřad malý a také proto, že se zde nachází mnoho problémů, které je třeba vyřešit. Všechny části, které budou podrobeny ISMS jsou v budově obecního úřadu a budeme se zaměřovat především na ICT.

Rozsah aktiv:

- obecní účetnictví
- seznam telefonních čísel
- databáze dodavatelů
- databáze ostatních institucí
- databáze předpřipravených dokumentů
- jednotlivé pracovní stanice
- databáze povinně zveřejňovaných dokumentů
- evidence mezd
- evidence obyvatel
- inventarizace majetku
- uložené zprávy z datové schránky
- evidence hřbitova

Příklad ostatních aktiv mimo budovu obecního úřadu

- obecní traktory
- obecní sekačky (traktůrky)
- vybavení obecní dílny

Převážně tato aktiva budou obsažena v ISMS. Odpovědnost za všechny aktiva nese starosta obce. Prvotní odpovědnost za účetnictví a evidenci mezd nese účetní. Odpovědnost za obecní traktory, sekačky a vybavení dílny nesou ostatní zaměstnanci obce, které obec zaměstnává z úřadu práce.

5.1.2 Politika ISMS

Obsahuje vizi obce v oblasti bezpečnosti informací. Starosta obce v politice ISMS také uvádí svůj zájem o zvýšení bezpečnosti v obci. Dokument o politice ISMS musí vydat sám obecní úřad, musí se s ním všichni zaměstnanci seznámit a musí být k němu umožněn volný přístup. V dokumentu se obec zaváže k:

- vytváření podmínek k zajišťování zdrojů potřebných k zavedení, udržení a zlepšování ISMS
- tomu, že bude uplatňována politika založená na principech dostupnosti, důvěrnosti a úplnosti informací, na požadavcích zainteresovaných stran a na požadavcích právních předpisů
- že bude pravidelně hodnotit splňování cílů a cílových hodnot, které vychází z analýzy rizik
- že bude neustále zvyšovat informovanost zaměstnanců obce o informační bezpečnosti
- tomu, že díky ISMS bude všem občanům a svým zaměstnancům zajišťovat dostatečnou jistotu bezpečnosti při používání jejich informací a dat

V rámci politiky ISMS se musí vybrat sponzor projektu. Tím by zde měl být starosta obce, který za všechno nese odpovědnost vůči státu a občanům a rovněž má také

největší přehled o dění na obecním úřadě v rámci použitých technologiích, o jeho zabezpečení a o požadavcích na bezpečnost.

5.1.3 Plán zvládání rizik

Další nutností je vytvoření plánu na zvládání rizik. Tento plán bude obsahovat pouze krátkodobé cíle podle ČSN ISO/IEC 27001 přílohy A. V plánu musí být rovněž uvedeno, kteří zaměstnanci jsou za identifikaci rizik a vytvoření opatření zodpovědní. Plán rizik se týká oblasti:

- Fyzické bezpečnosti a bezpečného prostředí
- Bezpečnosti provozu informačních technologií a informačních systémů
- Bezpečnost lidských zdrojů
- Zvládání kontinuity činností a incidentů
- Souhlas se zákonnými požadavky

Vlastníkem aktiv bude stanoven starosta obce, protože v konečném důsledku má za všechny aktiva v obci zodpovědnost. Bude tedy zodpovědný i za realizaci opatření podle ČSN ISO/IEC 27001 přílohy A. Tyto činnosti budou popsány v dalších kapitolách.

U všech opatření se uvede:

- osoba, která je odpovědná
- popis, jak se bude realizovat
- případná další dokumentace a odkazy na ní
- okamžik kdy bude proveden další krok
- odhad velikosti použitých zdrojů (finančních i personálních)

5.1.4 Metodika hodnocení rizik

Metodika hodnocení rizik vychází z ČSN ISO/IEC 27005:2006.

K zajištění základních požadavků na aktiva se musí brát ohled na možnost dopadu na zvolená aktiva při porušení bezpečnosti.

V obci se stanoví stupnice hodnocení aktiv.

Tabulka 1 Stupnice hodnocení aktiv v obci

Hodnota aktiv	Dopad na aktivum
zanedbatelná - 1	**Zanedbatelný dopad na aktivum**
	Nedošlo k zanedbání právních norem
	Možná škoda se neprojevuje v okolí obce.
	Náklady na odstranění či nápravu nepřesahují částku 50 000 Kč.
malá - 2	**Malý dopad na aktivum**
	Má negativní vliv na organizační celky, ale neprojeví se ve službách poskytovaných vně organizace
	Mohlo dojít k porušení právních norem a případné správní řízení nebo soudní pře mohou vést k finančnímu pokutě do částky 50 000 Kč
významná - 3	**Vážný dopad na aktivum**
	Správní řízení či soudní pře s postihem převyšuje 50 000 Kč.
	Může způsobit negativní publicitu v rámci oboru činnosti
	Újma způsobená jedné či více osobám mimo ohrožení zdraví či života.
	Má negativní vliv na oddělení organizace a dopad je promítnut do poskytovaných služeb.
velmi cenná - 4	**Velmi vážný dopad na aktivum**
	Ztráta důvěry jednoho nebo více obchodních partnerů.
	Značná finanční ztráta
	Potenciální nebezpečí zachování kontinuity podnikání.
	Veřejná negativní publicita.
	Vážné zranění či ohrožení života.

Zdroj: Vlastní zpracování z ČSN ISO/IEC 27005:2006 (10)

Aby byla zvolena vhodná opatření pro různá aktiva, je nutné vymezit úroveň hrozby, která se odvíjí od velikosti dopadu na aktiva a pravděpodobnost s jakou bude hrozba uskutečněna. Se stanovením hodnocení rizika se také určí úroveň hrozby, na kterou se provede retence nebo redukce.

Tabulka 2 Úroveň hrozeb

Úroveň hrozby	Hodnocení úrovně hrozby
Velmi nízká - VN	S velmi nízkou pravděpodobností může dojít k zanedbatelnému dopadu na činnost obce nebo její části.
	Možná akceptace rizika.
Nízká - N	Může dojít s nízkou pravděpodobností k zanedbatelnému dopadu na činnost obce nebo její části.

	Může dojít k malému dopadu na činnost obce nebo její části, ale s velmi nízkou pravděpodobností.
	Možná akceptace rizika.
Střední - S	Může dojít k malému dopadu na činnost obce nebo její části.
	Riziko se musí řešit.
Vysoká - V	Je velmi pravděpodobné, že může dojít k vážnému dopadu na činnost obce nebo její části.
	Riziko se musí řešit s vysokou prioritou.
Velmi vysoká - VV	Téměř jistě může dojít k velmi vážnému dopadu na činnost obce nebo její části.B10
	Riziko se musí řešit s nejvyšší prioritou.

Zdroj: Vlastní zpracování z ČSN ISO/IEC 27005:2006 (10)

Díky sestavené stupnici hodnot aktiv a úrovni hrozeb můžeme vytvořit jejich sloučením míru rizika. Z této míry rizika, která je vytvořena v následující tabulce se bude následně vycházet při zavádění ISMS do obce a to hlavně při zavádění opatření k odstranění hrozeb a rizik. Míra rizika může být nízká – N, střední – S nebo vysoká – V.

Tabulka 3 Míra rizika

Míra rizika		**Úroveň hrozby**				
		VN	**N**	**S**	**V**	**VV**
Hodnota aktiv	**1**	N - 1	N - 2	S - 3	S - 4	S - 5
	2	N - 2	S - 3	S - 4	S - 5	V - 6
	3	S - 3	S - 4	S - 5	V - 6	V - 7
	4	S - 4	S - 5	V - 6	V - 7	V - 8

Zdroj: Vlastní zpracování

Tabulka 4 Dopad hrozeb na dostupnost, důvěrnost a integritu

Aktivum	**Vliv na**		
	dostupnost	**důvěrnost**	**integritu**
účetnictví obce	3	4	4
databáze ostatních institucí	2	2	2
databáze dodavatelů	4	3	3
seznam telefonních kontaktů starosty	2	3	3
databáze předpřipravených dokumentů	4	3	4
jednotlivé pracovní stanice	3	2	2

databáze povinně zveřejňovaných dokumentů	2	3	2
evidence mezd	3	3	4
evidence obyvatel	3	3	3
inventarizace majetku	3	4	3
uložené zprávy z datové schránky	3	2	3
evidence hřbitova	3	2	2

Tabulka 5 Možné hrozby a jejich dopady

Hrozby		Dopad hrozby na		
		dostupnost	důvěrnost	integritu
Fyzické	Požár	4	4	3
	Vytopení	4	4	3
	Poničení okolními stromy	3	3	1
Výpadek služeb	Výpadek elektřiny	2	2	1
	Výpadek hlasové služby	3	3	1
	Výpadek internetu	2	2	1
	Výpadek webových služeb	2	2	1
	Výpadek emailové komunikace	3	3	1
Technické problémy	Porucha pracovní stanice	4	4	2
	Porucha USB disku	4	4	3
	Porucha externího disku	4	4	3
	Nefunkčnost Windows Vista	3	3	2
Selhání zaměstnanců	Nedodržování předpisů o práci s informacemi	2	3	3
	Špatná dokumentace systému	1	1	3
	Vyzrazení hesla	1	4	2
Nezákonná činnost	Neoprávněné vniknutí	2	3	2
	Neoprávněné kopírování dat	2	4	1
	Vyzrazení osobních údajů	1	4	1
Ohrožení důvěrnosti	Chyby v přístupových právech	3	4	2
	Slabá místa v zabezpečené síti	1	3	2
	Slabá místa v zabezpečení stanic	2	3	2
	Zranitelnost webových stránek	2	3	2
	Krádež USB disku	4	4	2
	Krádež USB tokenu	4	4	1

	Proniknutí škodlivého kódu	3	4	3
	Krádež technického zařízení	3	4	1

Tabulka 6 Míra identifikovaných rizik

Hrozby		databáze dodavatelů			seznam telefonních kontaktů starosty			databáze předpřipravených dokumentů			jednotlivé pracovní stanice			databáze povinně zveřejňovaných dokumentů			evidence mezd			evidence obyvatel			inventarizace majetku			uložené zprávy z datové schránky			evidence hřbitova		
		Do	Dů	In	Do	Dů	In	Do	Dů	In	Do	Dů	In	Do	Dů	In	Do	Dů	In	Do	Dů	In	Do	Dů	In	Do	Dů	In	Do	Dů	In	Do	Dů	In
Fyzické	Požár	8	7	6	6	7	6	8	7	7	7	6	5	6	7	5	7	7	7	7	7	6	7	8	6	7	6	6	7	6	5
	Vytopení	8	7	6	6	7	6	8	7	7	7	6	5	6	7	5	7	7	7	7	7	6	7	8	6	7	6	6	7	6	5
	Poničení okolními stromy	7	6	4	5	6	4	7	6	5	6	5	3	5	6	3	6	6	5	6	6	4	6	7	4	6	5	4	6	5	3
Výpadek služeb	Výpadek elektřiny	6	5	4	4	5	4	6	5	5	5	4	3	4	5	3	5	5	5	5	5	4	5	6	4	5	4	4	5	4	3
	Výpadek hlasové služby	7	6	4	5	6	4	7	6	5	6	5	3	5	6	3	6	6	5	6	6	4	6	7	4	6	5	4	6	5	3
	Výpadek internetu	6	5	4	4	5	4	6	5	5	5	4	3	4	5	3	5	5	5	5	5	4	5	6	4	5	4	4	5	4	3
	Výpadek webových služeb	6	5	4	4	5	4	6	5	5	5	4	3	4	5	3	5	5	5	5	5	4	5	6	4	5	4	4	5	4	3
	Výpadek emailové komunikace	7	6	4	5	6	4	7	6	5	6	5	3	5	6	3	6	6	5	6	6	4	6	7	4	6	5	4	6	5	3
Technické problémy	Porucha pracovní stanice	8	7	5	6	7	5	8	7	6	7	6	4	6	7	4	7	7	6	7	7	5	7	8	5	7	6	5	7	6	4
	Porucha USB disku	8	7	6	6	7	6	8	7	7	7	6	5	6	7	5	7	7	7	7	7	6	7	8	6	7	6	6	7	6	5
	Porucha externího disku	8	7	6	6	7	6	8	7	7	7	6	5	6	7	5	7	7	7	7	7	6	7	8	6	7	6	6	7	6	5
	Nefunkčnost Windows Vista	7	6	5	5	6	5	7	6	6	6	5	4	5	6	4	6	6	6	6	6	5	6	7	5	6	5	5	6	5	4
Selhání zaměstnanců	Nedodržování předpisů o práci s informacemi	6	6	6	4	6	6	6	6	7	5	5	5	4	6	5	5	6	7	5	6	6	5	7	6	5	5	6	5	5	5
	Špatná dokumentace systému	5	4	6	3	4	6	5	4	7	4	3	5	3	4	5	4	4	7	4	4	6	4	5	6	4	3	6	4	3	5

	Vyzrazení hesla	5	7	5	3	7	5	5	7	6	4	6	4	3	7	4	4	7	6	4	7	5	4	8	5	4	6	5	4	6	4
Nezákonná činnost	Neoprávněné vniknutí	6	6	5	4	6	5	6	6	6	5	5	4	4	6	4	5	6	6	5	6	5	5	7	5	5	5	5	5	5	4
	Neoprávněné kopírování dat	6	7	4	4	7	4	6	7	5	5	6	3	4	7	3	5	7	5	5	7	4	5	8	4	5	6	4	5	6	3
	Vyzrazení osobních údajů	5	7	4	3	7	4	5	7	5	4	6	3	3	7	3	4	7	5	4	7	4	4	8	4	4	6	4	4	6	3
Ohrožení důvěrnosti	Chyby v přístupových právech	7	7	5	5	7	5	7	7	6	6	6	4	5	7	4	6	7	6	6	7	5	6	8	5	6	6	5	6	6	4
	Slabá místa v zabezpečené síti	5	6	5	3	6	5	5	6	6	4	5	4	3	6	4	4	6	6	4	6	5	4	7	5	4	5	5	4	5	4
	Slabá místa v zabezpečení stanic	6	6	5	4	6	5	6	6	6	5	5	4	4	6	4	5	6	6	5	6	5	5	7	5	5	5	5	5	5	4
	Zranitelnost webových stránek	6	6	5	4	6	5	6	6	6	5	5	4	4	6	4	5	6	6	5	6	5	5	7	5	5	5	5	5	5	4
	Krádež USB disku	8	7	5	6	7	5	8	7	6	7	6	4	6	7	4	7	7	6	7	7	5	7	8	5	7	6	5	7	6	4
	Krádež USB tokenu	8	7	4	6	7	4	8	7	5	7	6	3	6	7	3	7	7	5	7	7	4	7	8	4	7	6	4	7	6	3
	Proniknutí škodlivého kódu	7	7	6	5	7	6	7	7	7	6	6	5	5	7	5	6	7	7	6	7	6	6	8	6	6	6	6	6	6	5
	Krádež technického zařízení	7	7	4	5	7	4	7	7	5	6	6	3	5	7	3	6	7	5	6	7	4	6	8	4	6	6	4	6	6	3

Tabulka 7 Výsledná hodnota rizik informačních aktiv

Hrozby		databáze dodavatelů	seznam telefonních kontaktů starosty	databáze předpřipravených dokumentů	jednotlivé pracovní stanice	databáze povinně zveřejňovaných dokumentů	evidence mezd	evidence obyvatel	inventarizace majetku	uložené zprávy z datové schránky	evidence hřbitova
Fyzické	Požár	8	7	8	7	7	7	7	8	7	7
	Vytopení	8	7	8	7	7	7	7	8	7	7
	Poničení okolními stromy	7	6	7	6	6	6	6	7	6	6
Výpadek služeb	Výpadek elektřiny	6	5	6	5	5	5	5	6	5	5
	Výpadek hlasové služby	7	6	7	6	6	6	6	7	6	6

	Výpadek internetu	6	5	6	5	5	5	5	6	5	5
	Výpadek webových služeb	6	5	6	5	5	5	5	6	5	5
	Výpadek emailové komunikace	7	6	7	6	6	6	6	7	6	6
Technické problémy	Porucha pracovní stanice	8	7	8	7	7	7	7	8	7	7
	Porucha USB disku	8	7	8	7	7	7	7	8	7	7
	Porucha externího disku	8	7	8	7	7	7	7	8	7	7
	Nefunkčnost Windows Vista	7	6	7	6	6	6	6	7	6	6
Selhání zaměstnanců	Nedodržování předpisů o práci s informacemi	6	6	7	5	6	7	6	7	6	5
	Špatná dokumentace systému	6	6	7	5	5	7	6	6	6	5
	Vyzrazení hesla	7	7	7	6	7	7	7	8	6	6
Nezákonná činnost	Neoprávněné vniknutí	6	6	6	5	6	6	6	7	5	5
	Neoprávněné kopírování dat	7	7	7	6	7	7	7	8	6	6
	Vyzrazení osobních údajů	7	7	7	6	7	7	7	8	6	6
Ohrožení důvěrnosti	Chyby v přístupových právech	7	7	7	6	7	7	7	8	6	6
	Slabá místa v zabezpečené síti	6	6	6	5	6	6	6	7	5	5
	Slabá místa v zabezpečení stanic	6	6	6	5	6	6	6	7	5	5
	Zranitelnost webových stránek	6	6	6	5	6	6	6	7	5	5
	Krádež USB disku	8	7	8	7	7	7	7	8	7	7
	Krádež USB tokenu	8	7	8	7	7	7	7	8	7	7
	Proniknutí škodlivého kódu	7	7	7	6	7	7	7	8	6	6
	Krádež technického zařízení	7	7	7	6	7	7	7	8	6	6

5.2 Zavedení ISMS v obci

V dalších podkapitolách bude uveden soubor opatření, který bude nutné zavést, nebo je revidovat tak, aby byla všechna identifikovaná rizika odstraněna, nebo dostatečně minimalizovaná a neměla tak dopad na informační aktiva obce.

Soubor opatření je převzat z ČSN ISO/IEC 27001:2006 a její přílohy A. U jednotlivých opatření bude uvedeno, zda budou použita či nikoli.

5.2.1 Soubor opatření dle ČSN ISO/IEC 27001:2006

Opatření jsou rozdělena do již zmíněných 11 oblastí, které se dělí na 34 kategorií a celkově je možno zavést 139 opatření, které v sobě obsahují ještě mnoho dalších kroků, které je třeba splnit k vytvoření opatření.

U každého opatření se rozhodne, zda bude opatření zavedeno nebo revidováno (v případě, že je již opatření uplatněno). Rozhodování bude probíhat na základě hodnocení rizik a bezpečnostní analýzy. V případě nevyužití některého z opatření bude tento postup odůvodněn.

Tabulka 8 Soubor opatření dle ČSN ISO/IEC 27005 a situace v obci

Oblast	Jednotlivá opatření	Situace	Odůvodnění
Bezpečnostní politika	Dokument bezpečnostní politiky informací	aplikovat	podporování procesů ISMS
	Přezkoumání bezpečnostní politiky informací	aplikovat	podporování procesů ISMS
Organizace bezpečnosti informací	Závazek vedení směrem k bezpečnosti informací	aplikovat	podporování procesů ISMS
	Koordinace bezpečnosti informací	aplikovat	podporování procesů ISMS
	Přidělení odpovědnosti v oblasti informační bezpečnosti	revidovat	podporování procesů ISMS
	Schvalovací proces prostředků pro zpracování informací	aplikovat	možné technické selhání, ztráta důvěrnosti
	Dohody o ochraně důvěrných informací	revidovat	neoprávněná činnost, ztráta důvěrnosti
	Kontakt s orgány veřejné správy	aplikováno	podporování procesů ISMS
	Kontakt se zájmovými skupinami		nekontaktují se žádné skupiny
	Nezávislá přezkoumání bezpečnosti informací		neprovádí se přezkoumání
	Identifikace rizik vyplývajících z přístupu externích subjektů	revidovat	neoprávněná činnost, ohrožení důvěrnosti
	Bezpečnostní požadavky pro přístup klientů		Občané nemají samovolný přístup k aktivům
	Bezpečnostní požadavky v dohodách se třetí stranou	revidovat	neoprávněná činnost, ohrožení důvěrnosti
Řízení aktiv	Evidence aktiv	revidovat	podporování procesů ISMS
	Vlastnictví aktiv	revidovat	podporování procesů ISMS
	Přípustné použití aktiv	revidovat	neoprávněná činnost,

Oblast	Jednotlivá opatření	Situace	Odůvodnění
			ohrožení důvěrnosti
	Doporučení pro klasifikaci	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Označování a zacházení s informacemi	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
Bezpečnost lidských zdrojů	Role a odpovědnosti	revidovat	zajištění důvěrnosti a dostupnosti
	Prověřování	aplikovat	zajištění důvěrnosti
	Podmínky výkonu pracovní činnosti	revidovat	neoprávněná činnost
	Odpovědnost vedoucích zaměstnanců	aplikováno	neoprávněná činnost
	Bezpečnostní povědomí, vzdělávání a školení v oblasti bezpečnosti informací	aplikovat	neoprávněná činnost
	Disciplinární řízení	revidovat	neoprávněná činnost
	Odpovědnost při ukončení pracovního vztahu	revidovat	neoprávněná činnost, ohrožení důvěrnosti
	Navrácení zapůjčených prostředků	aplikováno	zajištění dostupnosti
	Odebrání přístupových práv	revidovat	neoprávněná činnost, ohrožení důvěrnosti
Fyzická bezpečnost a bezpečnost prostředí	Fyzický bezpečnostní perimetr	aplikováno	neoprávněná činnost, ohrožení důvěrnosti
	Fyzické kontroly vstupu osob		nelze kontrolovat občany při vstupu
	Zabezpečení kanceláří, místností a prostředků	aplikováno	neoprávněná činnost, ohrožení důvěrnosti
	Ochrana před hrozbami vnějšku a prostředí	aplikovat	mechanické poškození
	Práce v zabezpečených oblastech	revidovat	zajištění dostupnosti
	Veřejný přístup, prostory pro nakládku a vykládku	revidovat	neoprávněná činnost, ohrožení důvěrnosti
	Umístění zařízení a jeho ochrana	revidovat	neoprávněná činnost, ohrožení důvěrnosti
	Podpůrná zařízení	revidovat	ohrožení dostupnosti
	Bezpečnost kabelových rozvodů	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Údržba zařízení	aplikovat	mechanické poškození
	Bezpečnost zařízení mimo prostory organizace	aplikovat	neoprávněná činnost, ohrožení důvěrnosti

Oblast	Jednotlivá opatření	Situace	Odůvodnění
	Bezpečná likvidace nebo opakované použití zařízení	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Přemístění majetku	revidovat	neoprávněná činnost, ohrožení důvěrnosti
Řízení komunikací a řízení provozu	Dokumentace provozních postupů	aplikovat	lidské a technické selhání
	Řízení změn	aplikovat	technické selhání, ohrožení důvěrnosti
	Oddělení povinností	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Oddělení vývoje, testování a provozu	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Dodávky služeb	aplikovat	technické selhání, ohrožení důvěrnosti
	Monitorování a přezkoumávání služeb třetích stran	aplikovat	lidské a technické selhání, ohrožení důvěrnosti
	Řízení změn služeb poskytovaných třetími stranami	revidovat	technické selhání, ohrožení důvěrnosti
	Řízení kapacit	aplikovat	technické selhání
	Přejímaní systémů		systémy se nepřijímají
	Opatření na ochranu proti škodlivým programům	revidovat	neoprávněná činnost, ohrožení důvěrnosti
	Opatření na ochranu proti mobilním kódům	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Zálohování informací	aplikovat	ztráta dostupnosti, technické selhání, lidské selhání
	Síťová opatření	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Bezpečnost síťových služeb	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Správa výměnných počítačových médií	revidovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání
	Likvidace médií	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Postupy pro manipulaci s informacemi	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Bezpečnost systémové dokumentace	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Postupy a politiky při výměně informací a programů	aplikovat	neoprávněná činnost, ohrožení důvěrnosti

Oblast	Jednotlivá opatření	Situace	Odůvodnění
	Dohody o výměně informací a programů	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Bezpečnost médií při přepravě	aplikovat	ohrožení důvěrnosti a dostupnosti
	Elektronické zasílání zpráv	revidovat	ohrožení důvěrnosti
	Informační systémy organizace	revidovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání
	Elektronický obchod		neprovozuje se
	On-line transakce		neprovozuje se
	Veřejně přístupné informace	aplikováno	neoprávněná činnost
	Pořizování auditních záznamů	revidovat	neoprávněná činnost, ohrožení důvěrnosti
	Monitorování používaní systému	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání, technické selhání
	Ochrana vytvořených záznamů	aplikovat	neoprávněná činnost
	Administrátorský a operátorský deník	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Záznam selhání	aplikovat	technické a lidské selhání
	Synchronizace času	aplikovat	neoprávněná činnost
Řízení přístupu	Politika řízení přístupu	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Registrace uživatele	aplikovat	lidské selhání, neoprávněná činnost, ohrožení důvěrnosti
	Řízení privilegovaného přístupu	aplikovat	lidské selhání, neoprávněná činnost, ohrožení důvěrnosti
	Správa uživatelských hesel	aplikovat	lidské selhání, neoprávněná činnost, ohrožení důvěrnosti
	Přezkoumání přístupových práv uživatelů	aplikovat	lidské selhání, neoprávněná činnost, ohrožení důvěrnosti
	Používání hesel	revidovat	lidské selhání, neoprávněná činnost, ohrožení důvěrnosti
	Neobsluhovaná uživatelská zařízení	revidovat	lidské selhání, neoprávněná činnost, ohrožení důvěrnosti
	Zásada prázdného stolu a prázdné obrazovky monitoru	aplikovat	lidské selhání, neoprávněná činnost, ohrožení důvěrnosti
	Politika užívání síťových služeb	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Autentizace uživatele pro externí připojení		zajišťuje dodavatel služeb
	Identifikace zařízení v sítích	revidovat	neoprávněná činnost,

Oblast	Jednotlivá opatření	Situace	Odůvodnění
			ohrožení důvěrnosti
	Ochrana portů pro vzdálenou diagnostiku a konfiguraci		zajišťuje dodavatel služeb
	Princip oddělení v sítích		zajišťuje dodavatel služeb
	Řízení síťových spojení		zajišťuje dodavatel služeb
	Řízení směrování sítě		zajišťuje dodavatel služeb
	Bezpečné postupy přihlášení	revidovat	neoprávněná činnost, ohrožení důvěrnosti
	Identifikace a autentizace uživatelů	revidovat	neoprávněná činnost, ohrožení důvěrnosti
	Systém správy hesel	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Použití systémových nástrojů	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Časové omezení relace	aplikovat	ohrožení důvěrnosti
	Časové omezení spojení	aplikovat	ohrožení důvěrnosti
	Omezení přístupu k informacím	revidovat	ohrožení důvěrnosti
	Oddělení citlivých systémů	aplikovat	ohrožení důvěrnosti
	Mobilní výpočetní zařízení a sdělovací technika		nevyužívá se
	Práce na dálku	revidovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání
Akvizice, vývoj a údržba informačních systémů	Analýza a specifikace bezpečnostních požadavků	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání
	Validace vstupních dat		neprovádí se
	Kontrola vnitřního zpracování		neprovádí se
	Integrita zpráv		neprovádí se
	Validace výstupních dat		neprovádí se
	Politika pro použití kryptografických kontrol		neprovádí se
	Správa klíčů		neprovádí se
	Správa provozního programového vybavení	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání
	Ochrana dat pro testování systému		neprovádí se
	Řízení přístupu ke knihovně zdrojových kódů		neprovádí se
	Postupy řízení změn	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, lidské

Oblast	Jednotlivá opatření	Situace	Odůvodnění
			selhání, technické selhání
	Technické přezkoumání aplikací po změnách operačního systému	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, ztráta služeb
	Omezení změn programových balíků	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání, technické selhání
	Unik informací	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání, technické selhání
	Programové vybavení vyvíjené externím dodavatelem	revidovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání, technické selhání
	Řízení, správa a kontrola technických zranitelností	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání, technické selhání
Zvládání bezpečnostních incidentů	Hlášení bezpečnostních událostí	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání
	Hlášení bezpečnostních slabin	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání
	Odpovědnosti a postupy reakce na incidenty	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání
	Ponaučení z bezpečnostních incidentů	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání
	Shromažďování důkazů	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání
Řízení kontinuity činností organizace	Zařazení informační bezpečnosti do procesu řízení kontinuity činností organizace	aplikovat	podporování procesů ISMS
	Kontinuita činností organizace a hodnocení rizik	aplikovat	podporování procesů ISMS
	Vytváření a implementace plánů kontinuity	aplikovat	ztráta dostupnosti, technické selhání, lidské selhání, fyzické poškození
	Systém plánování kontinuity činností organizace	aplikovat	ztráta dostupnosti, technické selhání, lidské selhání, fyzické poškození
	Testování, udržování a přezkoumávání plánů kontinuity	aplikovat	technické a lidské selhání

Oblast	Jednotlivá opatření	Situace	Odůvodnění
Soulad s požadavky	Identifikace odpovídajících předpisů	revidovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání
	Ochrana duševního vlastnictví	aplikovat	neoprávněná činnost, ohrožení důvěrnosti
	Ochrana záznamů organizace	revidovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání
	Ochrana dat a soukromích osobních údajů	aplikováno	neoprávněná činnost, ohrožení důvěrnosti
	Prevence zneužití prostředků pro zpracování informací	aplikovat	neoprávněná činnost, ohrožení důvěrnosti, lidské selhání
	Regulace kryptografických opatření		nevyužívá se
	Shoda s bezpečnostními politikami a normami	aplikovat	podporování procesů ISMS
	Kontrola technické shody	aplikovat	podporování procesů ISMS
	Opatření k auditu	revidovat	neoprávněná činnost, ohrožení důvěrnosti
	Ochrana nástrojů pro audit	aplikovat	neoprávněná činnost, ohrožení důvěrnosti

Zdroj: Vlastní zpracování (11)

5.2.2 Plán zavedení opatření

Vzhledem k tomu, že je obec poměrně malá, nemá tak velké zdroje, kterými by mohla pokrýt zavedení opatření v krátkém čase. Rovněž v současnosti neusiluje o certifikát systému ISMS, což by vyžadovalo rychlejší zavedení všech opatření. Díky těmto okolnostem lze zavedení opatření rozdělit na části a na delší časové období podle vhodnosti. Opatření na rizika se budou provádět akceptací rizika (nejsou provedeny žádné akce, riziko je identifikováno, ale považuje se za akceptovatelné, jeho hodnota v analýze rizik se pohybuje od 0-2) a redukcí rizika (odstraní se příčiny vzniku rizika nebo dopad rizika, riziko je přesunuto na další subjekty, provede se pojištění proti následkům rizika, nebo se zavedou vhodná opatření ke snížení, nebo úplnému odstranění rizika).

Časové fáze:

1. fáze proběhne v období 1. července až 31. prosince 2013. V prvních měsících budou provedeny převážně stavební úpravy, kterými se budou provádět opatření na fyzickou bezpečnost a bezpečnost prostředí. V následujících měsících bude řešena bezpečnostní politika informací. Do této fáze je nutné také zahrnout alespoň jedno opatření ze skupiny bezpečnosti lidských zdrojů, které se týká informovanosti, vzdělávání a školení zaměstnanců.
2. fáze proběhne v období 1. leden až 31. srpna 2014. Zde budou prováděna ostatní opatření na bezpečnost lidských zdrojů, opatření na organizaci bezpečnosti informací, řízení aktiv, řízení komunikace a řízení provozu a řízení kontinuity činností organizace.
3. fáze proběhne od 1. září do 31. března 2015. V tomto posledním období budou zavedena opatření na akvizici, vývoj a údržbu informačních systémů, na soulad s požadavky a na zvládání bezpečnostních incidentů a řízení přístupu.

Tento časový plán by měl být uskutečnitelný. Časová vytíženost zaměstnanců obecního úřadu je vždy koncem roku při provádění inventarizací a uzavírání účetnictví. Proto je na tyto etapy stanoveno více času. Během roku je prováděn audit, který je do plánu také započítán. Samozřejmě může nastat během následujících časových úseků nepředvídatelná událost, která zabere zaměstnancům mnoho času. Je tedy možné tyto úseky v případě nutnosti posunout a prodloužit termíny dokončení.

5.3 1. fáze opatření ISMS

V předchozích kapitolách byla splněna nezbytná součást zavádění ISMS, a to ustanovení ISMS a vytvoření politiky ISMS. Po vytvoření těchto kroků lze přistoupit k řízení bezpečnosti informací, a to zavedením opatření k redukci rizik.
V první fázi opatření ISMS bude řešeno jedno opatření z bezpečnosti lidských zdrojů a dále skupiny opatření fyzické bezpečnosti a bezpečnosti prostředí a dále to bude bezpečnostní politika informací.

5.3.1 Bezpečnost lidských zdrojů

Cílem opatření ve skupině bezpečnosti lidských zdrojů je již v počáteční fázi zajistit, aby byli zaměstnanci obecního úřadu dostatečně informováni, vzděláni a školeni v oblasti bezpečnosti informací. Ostatní opatření z této skupiny lze zavést v 2. fázi.

Informovanost, vzdělávání a školení zaměstnanců

Odpovědná osoba: starosta

Zdroje opatření:

- Pravidelné školení zaměstnanců obce 24 hodin/rok
- Poplatek za školení 8700 Kč

Opatření: Zaměstnanci obce a případně i pracovníci smluvních a třetích stran, musí s ohledem na vykonávanou činnost absolvovat vhodné a pravidelně se opakující školení v oblasti bezpečnosti informací, bezpečnostní politiky a směrnic obce. To zaručí informovanost zaměstnanců o prováděných změnách.

5.3.2 Fyzická bezpečnost a bezpečnost prostředí

Cílem opatření fyzické bezpečnosti a bezpečnosti prostředí je zajistit, aby nebyl umožněn neautorizovaný přístup a aby se předcházelo zásahům a poškozením do informací podniku.

Fyzický bezpečnostní perimetr

Odpovědná osoba: starosta

Zdroje opatření:

- Vytvoření dokumentace o perimetru 6 hodin
- Kontrola historie přístupů 0,5 hodin/týden

Opatření: Na obecním úřadě je již aplikováno opatření ve formě zabezpečení jednotlivých místností bezpečnostním systémem. 1. příchozí zaměstnanec musí systém odkódovat, aby byl možný přístup. Následně poslední odcházející zaměstnanec systém musí opět zakódovat. Bezpečnostní perimetr je stanoven již zavedeným bezpečnostním systémem, ale není nikde zdokumentován. Je tedy třeba vytvořit dokumentaci o

perimetru a také kontrolovat historii přístupů, a tak případně dohledat, že v průběhu oběda nebo noci, kdy na obecním úřadě nikdo není, došlo k zabezpečení prostoru.

Fyzická kontrola vstupu osob

Odpovědná osoba: starosta

Zdroje opatření:

- Dokumentace úředních hodin 0,5 hodiny
- Kontrola bezpečnostního systému v obci 1 hodina/měsíc

Opatření: Je třeba rozlišit fyzickou kontrolu vstupu osob při úředních hodinách a v ostatním čase. V případě úředních hodin je na obecní úřad volný přístup a v ostatních časech je prováděna kontrola pomocí bezpečnostního systému v obci. Je zde třeba vytvořit dokumentaci úředních hodin a provádět kontrolu bezpečnostního systému vždy jednou za měsíc.

Zabezpečení kanceláří, místností a prostředků

Odpovědná osoba: starosta

Zdroje opatření:

- Zámky na počítačové stanice 1200 Kč
- Vytvoření dokumentace k evidenci výpůjček klíčů 1 hodina
- Úprava konzolí stolu 500 Kč
- Uzamknutí počítačů 2 hodiny

Opatření: Vstupní dveře jsou zajištěny koulí a v případě neúředních hodin lze dveře přepnout do polohy zamčeno. Na počítačové vybavení je nutné zakoupit zámky, které se spojí s pevnou konzolí stolu. Klíče je třeba umístit do trezoru a vytvořit dokumentaci, kdy si kdo klíče půjčoval.

Ochrana před hrozbami vnějšku a prostředí

Odpovědná osoba: starosta

Zdroje opatření:

- Vytvoření požární signalizace 11 000 Kč
- Prořezání stromů 2 000 Kč

- Pravidelná roční kontrola stromů 500 Kč
- Pojištění obecního úřadu proti požáru 450 Kč/rok

Opatření: Nebezpečí povodně na obecním úřadě nehrozí. Je zde ale hrozba požáru. V místnosti se nachází množství elektroniky a množství dokumentů, které by mohly vzplanout. Proto je nutné vytvořit systém požární signalizace, která by byla napojena na požární zbrojnici v budově a rovněž na požární systém obce. Při vzniku požáru by se měla rovněž pověřeným osobám (starostovi obce, starostovi SDH Kaliště, účetní) odeslat varovná SMS.
Další vnější hrozbou je možnost pádu z jednoho ze vzrostlých stromů na budovu obecního úřadu. Opatření na tuto hrozbu je prořezání stromů a jeho pravidelná kontrola, která by se měla zaznamenávat do kontrolní dokumentace.
Proti vzniku požáru by bylo vhodné prozatím obecní úřad pojistit.

Práce v zabezpečených oblastech

Odpovědná osoba: starosta

Zdroje opatření:

- Kontrola dokumentace vypůjčených klíčů 1hodina/týden

Opatření: Pro přístup do zabezpečených oblastí, které obec vlastní, bude použit systém vypůjčování klíčů, které jsou umístěny v obecním trezoru. Jejich vypůjčení musí být dokumentováno.

Veřejný přístup, prostory pro nakládku a vykládku

Odpovědná osoba: starosta

Zdroje opatření:

- Jsou uvedeny v opatření pro fyzickou kontrolu vstupu osob

Opatření: Do prostor obecního úřadu lze vstoupit dvěma vchody. Jejich zabezpečení je odlišné. Lze tedy vstoupit vchodem přes hostinec a dostat se ke dveřím k obecnímu úřadu, které jsou zamčeny a místnost je zabezpečena. Při vstupu osob mimo úřední hodiny do obecního úřadu je nutný doprovod starosty obce nebo účetní.

V době úředních hodin je umožněn veřejný přístup a jako ohlášení vstupu je v kanceláři účetní implementován „bzučák“.

Umístění zařízení a jeho ochrana

Odpovědná osoba: starosta

Zdroje opatření: jsou řešeny v ochraně před hrozbami vnějšku a prostředí a v práci v zabezpečených oblastech.

Opatření: Zařízení jsou umístěna na zabezpečených místech, kam není umožněn přístup občanům bez doprovodu mimo úřední hodiny a v úřední hodiny je umožněn volný přístup, ale zaměstnanci jsou na vstup osoby předčasně informováni. Rovněž je zabezpečen přesun těchto zařízení díky zámku s konstrukcí stolu, který zabraňuje i případnému pádu monitorů.

Podpůrná zařízení

Odpovědná osoba: starosta

Zdroje opatření:

- Přepěťová ochrana 3000 Kč
- Zdroj UPS pro pracovní stanice 12000 Kč
- Zdroj UPS pro ostatní prvky 2000 Kč

Opatření: Pro všechny počítače bude zajištěn nepřerušený přívod energie pomocí zdrojů UPS. Protože je zavedena přepěťová ochrana pouze na jedné pracovní stanici, bude dokoupena i pro ostatní pracovní stanice a aktivní prvky. Dále bude přepěťová ochrana zabezpečovat rovněž konektivitu do internetu.

Bezpečnost kabelových rozvodů

Odpovědná osoba: starosta

Zdroje opatření:

- Pořízení bezpečnostních žlabů 2200 Kč
- Instalace žlabů 1200 Kč

Opatření: Kabelové rozvody a vedení kabelů bude zajištěno pomocí bezpečnostních žlabů, kterými budou nahrazeny současné žlaby. Vedení, které nebylo zakryto, bude rovněž umístěno do bezpečnostních žlabů.

Údržba zařízení

Odpovědná osoba: starosta

Zdroje opatření:

- Vytvoření plánu pro opakované revize 3 hodiny
- Kontrola pracovních stanic a jiného zařízení 1000 Kč/měsíc
- Kontrola zdrojů UPS 8 hodin/měsíc

Opatření: Je nutné vypracovat plán pro opakované revize všech počítačů a ostatního zařízení. Za revizi bude zodpovědný externě najatý pracovník. O provedených revizích budou zapsány záznamy a při zjištěných nedostatcích bude informován starosta obce, který zajistí nápravu. Tato náprava bude provedena externím pracovníkem nebo jiným možným řešením. Při revizi pracovních stanic budou tyto stanice očištěny od prachu.
Bude prováděna pravidelná kontrola zakoupených zdrojů UPS po 2 měsících a záznamy o výsledcích budou dokumentovány.

Bezpečnost zařízení mimo prostory organizace

Odpovědná osoba: starosta

Zdroje opatření:

- Vytvoření pravidel používání 8 hodin

Opatření: Pro zařízení, která se používají mimo obecní úřad, se musí stanovit pravidla používání, způsob ochrany a stanovit odpovědnost za možné problémy. Zaměstnanci obecního úřadu s těmito pravidly musí být seznámeni.

Bezpečná likvidace nebo opakované použití zařízení

Odpovědná osoba: starosta

Zdroje opatření:

- Vypracování postupů likvidace 3 hodiny

- Nákup softwaru na skartování dat 1000 Kč
- Nákup skartovacího zařízení na nosiče CD/DVD 800 Kč

Opatření: Vytvoří se postupy likvidace zařízení, na kterých jsou zaznamenána chráněná data a informace. Stanoví se osoba, která takto může zařízení znehodnotit a bude o všech znehodnocených nosičích provádět záznam. V postupu likvidace bude stanoven software, kterým budou data skartována a bude zakoupeno skartovací zařízení i na nosiče CD/DVD.

Přemístění majetku

Odpovědná osoba: odpovědný vlastník aktiva

Zdroje opatření:

- Vytvoření směrnice pro přemisťování majetku 3 hodiny
- Kontrola přesunutých aktiv ze záznamů 2 hodiny/měsíc

Opatření: Pro přemístění majetku je rovněž zavedena směrnice, jak tuto činnost provést. Pro přesunutí aktiva je nutný souhlas vlastníka tohoto aktiva, který zaznamená, kam a kdy bylo aktivum přesunuto a za jakým účelem. Všichni zaměstnanci obecního úřadu musí být seznámeni se směrnicí.

5.3.3 Bezpečnostní politika informací

Cílem opatření bezpečnostní politiky informací je vyjádřit podporu starosty obce k zavedení požadavků obce k tomu, aby byly splněny náležitosti souvisejících zákonů a norem, v případě certifikace.

Dokument bezpečnostní politiky informací

Odpovědná osoba: starosta

Zdroje opatření:

- Vytvoření bezpečnostní politiky obce 32 hodin
- Seznámení ostatních s vytvořenou politikou 4 hodiny

Opatření: Starosta musí vytvořit bezpečnostní politiku obce. Následně jsou s touto politikou seznámeni všichni zaměstnanci obecního úřadu a všichni členové zastupitelstva a místostarosta.

Přezkoumání bezpečnostní politiky informací

Odpovědná osoba: starosta

Zdroje opatření:

- Sestavení plánu na přezkoumání bezpečnostní politiky 4 hodiny
- Přezkoumání bezpečnostní politiky a její úpravy 18 hodin/rok

Opatření: U vytvořené bezpečností politiky v obci se bude v pravidelných intervalech přezkoumávat její účinnost. Protože je obecní úřad poměrně malý, kontroly se budou provádět jednou ročně. Po delším sžití zaměstnanců s bezpečnostní politikou se interval kontroly zkrátí na období 3 měsíců. Při každé kontrole se zjišťuje, zda je bezpečnostní politika dobře nastavena. V případě možných zlepšení se provede aktualizace bezpečnostní politiky.

5.4 Zdroje pro 1. fázi zavedení opatření

V první fázi zavedených opatření jsou řešena opatření bezpečnosti lidských zdrojů, bezpečnostní politiky informací a opatření na fyzickou bezpečnost a bezpečnost prostředí. Opatření na bezpečnostní politiku informací a bezpečnosti lidských zdrojů jsou základem pro další vznikající opatření. Opatření na fyzickou bezpečnost a bezpečnost prostředí byly zavedeny v 1. fázi, protože v nich je zahrnuta částečná přestavba, vylepšení současných zařízení a dovybavení dalším zařízením.

Provádění první fáze by nemělo významně narušit možnost vykonávání běžných úkonů pracovníků obecního úřadu.

U vypsaných opatření byly uvedeny finanční a lidské zdroje nutné k provedení těchto zmíněných opatření. Celkovým sečtením těchto zdrojů stanovíme celkové náklady na zavedení první fáze.

Tabulka 9 Náklady 1. fáze zavedených opatření

Opatření	Dílčí opatření	Lidské zdroje		Finanční zdroj	
		jednorázové	opakované (přepočtené za rok)	jednorázové	opakované (přepočtené za rok)
Informovanost, vzdělávání a školení zaměstnanců	Pravidelné školení zaměstnanců obce		24		
	Poplatek za školení				8 700 Kč
Dokument bezpečnostní politiky informací	Vytvoření bezpečnostní politiky obce	32			
	Seznámení ostatních s vytvořenou politikou	4			
Přezkoumání bezpečnostní politiky informací	Sestavení plánu na přezkoumání bezpečnostní politiky	4			
	Přezkoumání bezpečnostní politiky a její úpravy		18		
Fyzický bezpečnostní perimetr	Vytvoření dokumentace o perimetru	6			
	Kontrola historie přístupů		26		
Fyzické kontroly vstupu osob	Dokumentace úředních hodin	0,5			
	Kontrola bezpečnostního systému v obci		12		
Zabezpečení kanceláří, místností a prostředků	Zámky na počítačové stanice			1 200 Kč	
	Vytvoření dokumentace k evidenci výpůjček klíčů	1			
	Úprava konzolí stolu			500 Kč	
	Uzamknutí počítačů	2			
Ochrana před hrozbami vnějšku a prostředí	Vytvoření požární signalizace			11 000 Kč	
	Prořezání stromů			2 000 Kč	
	Pravidelná roční kontrola stromů				500 Kč
	Pojištění obecního úřadu proti požáru				450 Kč

Opatření	Dílčí opatření	Lidské zdroje		Finanční zdroj	
		jednorázové	opakované (přepočtené za rok)	jednorázové	opakované (přepočtené za rok)
Práce v zabezpečených oblastech	Kontrola dokumentace vypůjčených klíčů		52		
Podpůrná zařízení	Přepěťová ochrana			3 000 Kč	
	Zdroj UPS pro pracovní stanice			12 000 Kč	
	Zdroj UPS pro ostatní prvky			2 000 Kč	
Bezpečnost kabelových rozvodů	Pořízení bezpečnostních žlabů			2 200 Kč	
	Instalace žlabů			1 200 Kč	
Údržba zařízení	Vytvoření plánu pro opakované revize	3			
	Kontrola pracovních stanic a jiného zařízení				12 000 Kč
	Kontrola zdrojů UPS		96		
Bezpečnost zařízení mimo prostory organizace	Vytvoření pravidel používání	8			
Bezpečná likvidace nebo opakované použití zařízení	Vypracování postupů likvidace	3			
	Nákup softwaru na skartování dat			1 000 Kč	
	Nákup skartovacího zařízení na nosiče CD/DVD			800 Kč	
Přemístění majetku	Vytvoření směrnice pro přemisťování majetku	3			
	Kontrola přesunutých aktiv ze záznamů		24		
Celkem		**66,5**	**252**	**36 900 Kč**	**21 650 Kč**

Tabulka 10 Součet nákladů na 1. fázi opatření

Jednorázové finanční náklady	36 900 Kč

Opakované finanční náklady	21 650 Kč
Náklady na jednorázové mzdy * 220 Kč/hod	14 630 Kč
Náklady na opakované mzdy * 220 Kč/hod	55 440 Kč
Celkem	**128 620 Kč**

Za všechna stanovena opatření, která budou zavedena v 1. fázi obec zaplatí 128 620 Kč. Vzhledem k tomu, že obec není velká a nedostává přiděleno tolik finančních prostředků do svého rozpočtu, jako velké obce, nemůže si dovolit provádět mnoho opatření během jednoho roku. Proto bylo zavedení opatření rozděleno do 3. fází, které by měly být dokončeny 31. března 2015.

5.5 Přezkoumávání, monitorování, zlepšování a udržování ISMS

Při vytvoření bezpečnostní politiky v obci a při vyjádření podpory starosty obce k řešení bezpečnosti informací se spouští koloběh soustavného procesu ISMS.

Proces ISMS není nikdy ukončen a stále dochází k jeho zlepšování podle Demingova cyklu PDCA.

Podle zavedených opatření sepsaných v ČSN ISO/IEC 27001:2006 se u všech opatření stanovují plány pravidelných kontrol a monitorování bezpečnostních incidentů. Je vhodné, když jsou odpovědní pracovníci dostatečně seznámeni s důležitostí bezpečnosti informací a snaží se vyhledávat nové možné hrozby, ze kterých mohou vzniknout další rizika.

V oblasti ICT je oproti jiným odvětvím charakteristický rychlý růst. Rozvíjí se také v mnohem větší míře znalosti lidí v tomto odvětví a díky těmto znalostem je možnost, že vniknou do našeho či jiného systému. Proti těmto novým hrozbám je třeba se neustále chránit a využívat proaktivní přístup. Jednou z možností využití tohoto přístupu je umožnit zaměstnancům, kteří mají bezpečnost na starost, aby se vzdělávali v novinkách týkajících se bezpečnosti a tím zlepšovali náš systém ISMS.

6 Závěr

Tato diplomová práce je tvořena ze dvou hlavních částí. První část je teoretická a je v ní popsána metodika řešení bezpečnosti informačních technologií pro různé organizace.
Ze začátku jsou vysvětleny základní pojmy a procesy týkající se bezpečnosti informací, dále zákony a normy. Popsané normy jsou především normy řady ISO/IEC 27000:2006. Je kladen důraz na popsání politiky bezpečnosti informací v organizaci a opatření, která se zavádí při ISMS podle české technické normy ISO/IEC 27001:2006.

Druhá část diplomové práce je zaměřena na zavedení ISMS do zvolené obce. Nejprve byla podrobně popsána zvolená obec a následně situace v obci zanalyzována, aby se zjistily možné hrozby a rizika, na které je třeba reagovat.

Po provedené analýze bylo pro obec navrženo několik opatření, která by bylo dobré zavést, aby se snížil dopad možných rizik. Proces zavedení opatření byl rozdělen do tří fází, které byly časově rozvrženy.

Podrobně bylo v druhé části práce popsáno zavedení opatření v první fázi. Ta by měla obsahovat především opatření pro bezpečnostní politiku informací, bezpečnost lidských zdrojů a fyzickou bezpečnost a bezpečnost prostředí.
Ke každému opatření byly sepsány potřebné lidské a finanční zdroje. Tyto zdroje byly sečteny a pro zavedení opatření v první etapě obec bude potřebovat 128 620 Kč.

Jak je vidět, tato částka je pro obec poměrně významná vzhledem k velikosti rozpočtu obce. Tento fakt je tedy jedním z důvodů, proč bylo rozložení etap na zavedení opatření naplánováno až do 31. března roku 2015. Dalším důvodem, proč byly etapy rozloženy v tak dlouhém čase je, že obec v současnosti nepovažuje za důležité provést certifikaci ISMS.

Věřím, že tato diplomová práce bude pro řešení bezpečnosti informací v obci přínosem. Ten spočívá v tom, že obec ušetří finanční prostředky za provedení analýzy v obci a

určení rizik, které obci hrozí a také tím, že obec začne respektovat zmíněné hrozby a provede popsaná opatření, která by dopad hrozeb snížila.

7 Seznam použité literatury

1. **Palán, Zdeněk.** Systém. *Andromedia.cz.* [Online] [Citace: 15. 3. 2013.] http://www.andromedia.cz/andragogicky-slovnik/system.

2. **Doucek, P., a další, a další.** *Řízení bezpečnosti informací.* 2. rozšířené vydání. Příbram : Professional publishing, 2011. 286 s.. ISBN 978-80-7431-050-8.

3. **Tulloch, M.** *Microsoft Encyclopedia of Security.* Washington : Microsoft Press, 2003. 480 s. ISBN 0-7356-1877-1.

4. **Požár, J.** *Informační bezpečnost.* Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-3-8-5.

5. **Kný, M a Požár, J.** *Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti.* Brno : Tribun EU, 2010. ISBN 978-80-7399-067-1.

6. **Gregory, P.** *Enterprise Information Security for Non-Technical Decision Makers.* Harlow : Pearson Education Limited, 2003. 167 s. ISBN 0-273-66157-4.

7. **ČSN ISO/IEC 27001.** *Informační technologie - Bepečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.* Praha : Český normalizační institut, 2006.

8. **Smejkal, V. a Rais, K.** *Řízení rizik ve firmách a jiných organizacích.* 3. vyd. Praha : Grada Publishing, 2010. 360 s. ISBN 978-80-247-3051-6.

9. **Sedlák, Petr.** *Přiměřená bezpečnost.* [2. prezentace z předmětu Management informační bezpečnosti] Brno : VUT, 16. 1. 2013.

10. **ČSN ISO/IEC 27005:2006.** Česká technická norma. *Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.* [Online] 2006. [Citace: 18. 3. 2013.] http://csnonlinefirmy.unmz.cz/html_nahledy/36/83193/83193_nahled.htm.

11. **ČSN ISO/IEC 27002.** *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů.* Praha : Český normalizační institut, 2008.

8 Seznam obrázků a tabulek