Obsah

Úvod

Žijeme ve světě rizik, kdy vedle finančních, investičních či podnikatelských existují také rizika bezpečnostní. A právě tato rizika se dostávají do popředí zájmu, protože neustále roste podíl informací, které zpracováváme v té nejzranitelnější podobě – elektronicky. Hrozbou nejsou jen hackeři, útok může přijít zevnitř firmy v podobě nespokojených, podplacených nebo nezodpovědných zaměstnanců nedodržujících bezpečnostní pravidla. Důsledkem nemusí být „pouze“ krádež informací, ale i jejich nedostupnost či změna. K tomu lze připsat i další rizika jako rozesílání virů jménem firmy, manipulování s kontem v bance či nakupování na Internetu. Jednou důležitou oblastní informací jsou osobní údaje, jejichž ochrana nabývá na významu neboť jsou lehce zneužitelným artiklem.

Problematika mě zaujala natolik, že jsem si oblast ochrany osobních údajů vybrala jako téma své diplomové práce, a to v kontextu se zavedením inovačních postupů uvnitř organizace, které by měly napomoci osobní údaje odpovídajícím způsobem chránit. Prostudovala jsem dostupné literární prameny a využila vstřícnosti státní instituce, která mi umožnila nahlédnout do svých interních dokumentací, organizačních opatření, metodických pokynů a projektových podkladů.

Ústředním tématem práce je v širším slova smyslu bezpečnost zpracovávaných informací u organizace, v tomto případě u okresního státního zastupitelství. V užším slova smyslu se zaměřuje na ochranu osobních údajů v návaznosti na fyzickou, personální, administrativní a informační bezpečnost. V práci je nastíněn celý komplex důležitých prvků, které se významnou měrou podílejí na bezpečnosti informací státní instituce, a to vše v souvislosti s plněním povinností organizací vyplývajících ze zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Cílem diplomové práce je posouzení stavu přijatých opatření k ochraně osobních údajů, posouzení a zdokumentování možných rizik a vypracování návrhu nezbytných opatření k dosažení shody s platnou právní úpravou. Jedná se tedy o zmapování stávající situaci v oblasti ochrany osobních údajů u okresního státního zastupitelství. Záměrem nebyla detailní analýza, což z hlediska nedostupnosti některých materiálů nebylo ani možné, ale záměrem bylo pokusit se na základě studia dostupných pramenů najít rezervy a možnosti, jak zlepšit stav v oblasti ochrany informací, resp. osobních údajů.

V práci je popsána problematika bezpečnosti informací v souvislosti s bezpečnostní politikou jako základním dokumentem každé organizace. Jednotlivé části jsou pak věnovány komplexní ochraně a osobnosti manažera.

V další části práce je uveden přehled oblastí a cílů bezpečnosti, kterých má být dosaženo, dále pak popis současného stavu, kdy jsou hodnoceny jednotlivé oblasti bezpečnosti, kdy cíle slouží pouze pro jejich logickou kategorizaci.

V poslední části práce je provedeno vyhodnocení analýzy, včetně navržených řešení pro zvýšení bezpečnosti při ochraně informací státní instituce.

Prezentované závěry mohou být pomocným vodítkem pro vytváření strategií pro předcházení bezpečnostních incidentů organizace, a to nejen státní instituce, která je popsána v této práci. Diplomová práce může být současně využita pro vnitřní potřebu státního zastupitelství, jehož se týká.

1 Vymezení problému a cíle práce

Zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů (dále také „Zákon“) definuje povinnosti při ochraně osobních údajů (dále také „OOÚ“), ale **ponechává volnost v tom, jak tyto povinnosti naplnit**. Povinnosti stanovené v zákoně platí bez rozdílu pro všechny instituce jak ze sféry veřejné, tak soukromé. Státní dozor nad plněním ustanovení Zákona vykonává Úřad pro ochranu osobních údajů, který disponuje nástroji k vymahatelnosti práva, a to zejména formou peněžitých sankcí.
Osobní údaje jsou základním aktivem okresního státního zastupitelství, proto je problematika, řešená v této práci, ve světle uvedeného velmi aktuální.

Cílem diplomové práce bylo posouzení stávajícího stavu zavedených procesů při zpracování osobních údajů v listinné i elektronické podobě, posouzení a zdokumentování možných rizik. Dále pak na základě provedené analýzy rizik zpracovat návrh na zavedení nezbytných opatření k dosažení shody s platnou právní úpravou.

2 Teoretická východiska práce

2.1 Charakteristika organizace

Státní zastupitelství je významným činitelem výkonu spravedlnosti. Státní zastupitelství realizuje právo státu na stíhání osob, které se měly dopustit trestných činů. Tento zájem se v demokratické trestní justici chápe šířeji jako „veřejný zájem“, který je v tom, že veřejný žalobce stíhá osoby podezřelé ze spáchání trestného činu, ale i v tom, že veřejný žalobce má uloženy povinnosti k oběti trestného činu, mladistvým pachatelům, obhajobě ap. Tyto povinnosti se týkají ochrany základních práv a svobod, do nichž je zasahováno v trestním řízení, a to nejen obviněného, ale i dalších osob zúčastněných na trestním procesu. V konkrétní podobě se jedná např. o nepřípustnost zatajení důkazů ve prospěch obviněného, povinnost nepodat obžalobu za určitých skutkových předpokladů (např. podezření ve vztahu k obviněnému bylo vyvráceno), povinnost zamezit porušování práv a svobod ze strany policie v rámci stadia před podáním obžaloby. Státní zastupitelství zajišťuje veřejný zájem i v netrestní oblasti své působnosti.

Účast státních zástupců a soudců na výkonu trestní spravedlnosti je rozdílná. Soudci v trestním řízení rozhodují o vině a trestu, státní zástupci podávají k soudu obžalobu a zastupují ji v řízení před soudem. Pro plnění obžalovací funkce si zajišťují potřebné podklady v rámci předsoudního stadia trestního řízení. V předsoudním stadiu procesu uplatňují státní zástupci zájem státu na boji s trestnou činností. Rozdílné povaze činnosti v trestním řízení odpovídá jiné uspořádání státního zastupitelství oproti soustavě soudů (vyšší míra centralizace, závaznost pokynu nadřízeného). Společným rysem je to, že soudci i státní zástupci se účastní na výkonu trestní spravedlnosti.

Z výše uvedeného je tedy zřejmé, že se na státním zastupitelství pracuje s osobními údaji ve velkém množství a právě každodenní rutinní manipulace s nimi dává velký prostor pro jejich ztrátu, změnu, či zneužití. Z tohoto pohledu se jeví diplomová práce jako potřebná a smysluplná. (Nejvyšší státní zastupitelství)

Soustava státního zastupitelství

Organizační struktura státních zastupitelství v České republice je řešena monokraticky, podřízená je ministerstvu spravedlnosti. Na vrcholku této struktury je Nejvyšší státní zastupitelství se sídlem v Brně. Jemu jsou přímo podřízena vrchní státní zastupitelství v Praze a Olomouci. Těmto zastupitelstvím jsou podle rozhodnutí podřízena jednotlivá krajská státní zastupitelství s určitou modifikací v Praze, kde jsou na stejné úrovni Městské státní zastupitelství Praha a Krajské státní zastupitelství Praha. Nejnižší stupeň tvoří okresní (městská) státní zastupitelství, opět s výjimkou v Praze, kde jsou na stejné úrovni obvodní státní zastupitelství. Odpovědnost za jednotlivé organizační složky státu nesou vedoucí státní zástupci.

Ministerstvo vykonává správu Nejvyššího státního zastupitelství, vrchních, krajských a okresních státních zastupitelství tím, že:

- zajišťuje chod státních zastupitelství po stránce organizační, zejména stanoví počty státních zástupců a dalších zaměstnanců státních zastupitelství,
- zajišťuje chod státních zastupitelství po stránce personální v rozsahu stanoveném zákonem, řídí a kontroluje vedení personální agendy zajišťované vedoucími státními zástupci; ministr spravedlnosti jmenuje a odvolává náměstky vedoucích státních zastupitelství,
- zajišťuje chod státních zastupitelství po stránce finanční a hospodářské zejména tím, že zabezpečuje jejich finanční, materiální a technické potřeby, plní úkoly vyplývající z práva hospodaření s národním majetkem a provádí se revize hospodaření státních zastupitelství,
- organizuje, řídí a kontroluje výkon správy státních zastupitelství prováděný vedoucími jednotlivých státních zastupitelství.

Krajský státní zástupce vykonává správu krajského státního zastupitelství a správu okresních státních zastupitelství a jeho obvodu tím, že:

- zajišťuje jeho chod po stránce personální zejména tím, že zabezpečuje jeho řádné obsazení odbornými a dalšími zaměstnanci a vyřizuje personální věci státních zástupců a ostatních zaměstnanců těchto státních zastupitelství,
- zajišťuje chod krajského státního zastupitelství a okresních státních zastupitelství jeho obvodu po stránce hospodářské, materiální a finanční,

- zajišťuje chod okresních státních zastupitelství v jeho obvodu po stránce organizační, zejména tím, že na základě plánu pracovníků stanoveného ministerstvem, určuje počty státní zástupců a ostatních zaměstnanců těchto okresních státních zastupitelství.

Okresní státní zástupce se podílí na výkonu správy okresního státního zastupitelství v souladu s pokyny krajského státního zástupce. Dohlíží na plynulost řízení u okresního státního zastupitelství a na řádné plnění povinností státních zástupců, působících u tohoto státního zastupitelství.

Organizační schéma okresního státního zastupitelství, které bylo předmětem diplomové práce, je znázorněno v příloze č. 1.

2.2 Ochrana osobních údajů

Dne 7. června 2007 vyšel ve sbírce zákon č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru, který ve své třinácté části přinesl významné změny v ustanoveních zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Nejvýznamnější změny se týkají § 13, který stanoví povinnosti osob při zabezpečení osobních údajů, kde nově stanovuje povinnost posoudit rizika a zavádí některé nové povinnosti v oblasti automatizovaného zpracování osobních údajů.

Zákon rozlišuje osoby, které zpracovávají osobní údaje jiných lidí (tzv. správce nebo zpracovatel osobních údajů) a dále osoby, jejichž osobní údaje správce a zpracovatel zpracovávají (tzv. subjekty údajů). Na ochranu práv subjektů údajů a kontrole plnění povinností správce a zpracovatele osobních údajů byl zřízen Úřad na ochranu osobních údajů.

Za neplnění povinností stanovených správci nebo zpracovateli osobních údajů hrozí správci nebo zpracovateli osobních údajů sankce. Jednou z povinností, jež má správce osobních údajů plnit, je zveřejňovat na internetu informace o zpracování osobních údajů. Pro snadné plnění této povinnosti byla zřízena speciální webová stránka - Rejstřík správců osobních údajů.

Proč se zabývat ochranou osobních údajů?

- **Filosofická odpověď:** Ochrana osobních údajů je jedna ze součástí ochrany osobnosti. Pokud se k sobě mají lidé chovat slušně, pak by součástí tohoto slušného chování mělo být i odpovědně nakládat s jejich osobními údaji. Povinnosti stanovené zákonem na ochranu osobních údajů představují pouze uzákonění něčeho, co slušní lidé, kteří mají k dispozici osobní údaje jiných lidí, stejně dělají. Ochrana osobních údajů by tak měla být součástí lidské slušnosti.

- **Pragmatická odpověď:** Plnit povinnosti stanovené zákonem na ochranu osobních údajů je třeba, protože za jejich neplnění hrozí sankce. S těmito povinnostmi se člověk nemusí ztotožnit, může na ně nadávat, ale pokud je neplní, vystavuje se tak postihu. Je to obdobné jako placení daní. S ochranou osobních údajů je to v tomto

smyslu stejné jako s daněmi. Sankce za nerespektování ochrany osobních údajů jsou přitom ve srovnání se sankcemi za neplacení daní mnohem přísnější.

Jak začít s ochranou osobních údajů?

Základní ideou ochrany osobních údajů, která je promítnuta do povinností správce, je, že osobní údaje se zpracovávají za určitým účelem. K realizaci konkrétního účelu zpracování jsou potřeba pouze určité osobních údaje (co do množství, tak počtu lidí, jichž se týkají) a dále jsou potřebné pouze určité operace, jež se s osobními údaji provádějí. Základem je proto popis toho, k čemu správce osobní údaje má, kolik jich má, a co s nimi dělá. Zákon si pro to vytvořil speciální termíny jako je účel zpracování, prostředky zpracování, způsob zpracování, kategorie osobních údajů, kategorie subjektů údajů a kategorie příjemců. To je třeba popsat v termínech uvedených v zákoně. Je tedy třeba udělat audit osobních údajů (co jako správce mám a proč), roztřídit si tyto údaje podle účelu (podle toho, na co je potřebuji) a každý účel podrobně popsat v termínech, jež stanovuje zákon.

Sankce za nakládání s osobními údaji v rozporu se zákonem

Při nakládání s osobními údaji, které je v rozporu se zákonem, se mohou fyzické osoby dopustit přestupku případně trestného činu a právnické osoby a fyzické osoby podnikající jiného správního deliktu. Trestní odpovědnost osob, jež jednají za právnickou osobu tím není dotčena. Přestupky nebo trestné činy nejsou jenom doménou správce nebo zpracovatele osobních údajů, ale kohokoli, kdo s osobními údaji nějak nakládá. Jelikož je při nezákonném nakládání s osobními údaji porušeno právo na ochranu osobnosti člověka, jež chrání podstatné atributy lidské existence jako je např. soukromí, důstojnost, čest apod., jejichž náprava je obtížná, ne-li nemožná, jsou sankce za porušování povinností při nakládání s osobními údaji stanoveny poměrně přísně. (http://www.oou.cz)

2.3 Vybrané oblasti managementu

Vzhledem k tomu, že management v dnešní společnosti zasahuje do všech oblastí jejího života, vybrala jsem ta témata, která se nějakým způsobem týkají zaměření mé diplomové práce.

2.3.1 Podnikový management

Možné **definice** managementu (Němeček, Zich, 2006, 1. díl, s. 6):

- Management znamená vykonávání úkolů prostřednictvím práce jiných. *(American Management Asociation)*
- Management je vykonávání věcí prostřednictvím jiných lidí. *(E. Dalea, J. Hayse)*
- Management je proces vytváření určitého prostředí, ve kterém jednotlivci pracují společně ve skupinách, efektivně uskutečňují zvolené cíle. *(H. Koontz, H. Werich)*
- Management je proces plánování, organizování, vedení a kontroly organizačních činností zaměřených na dosažení organizačních cílů. *(K. H. Chung)*
- Management jsou typické činnosti, které manažer vykonává, jako je rozhodování, organizování, plánování, kontrolování, vedení lidí, koordinace, motivování atd. *(K. Muller)*
- Management je oblast studia, které se věnuje stanovení postupů, jak co nejlépe dosáhnout cílů organizace. *(S. P. Robins)*
- Management je proces optimalizace využití lidských, materiálních a finančních zdrojů k dosažení organizačních cílů. *(J. A. Pearce, R. B. Robinson)*
- Management je soubor přístupů, názorů, doporučení a metod, které vedoucí pracovníci (manažeři) užívají ke zvládnutí specifických činností (manažerských funkcí), směřujících k dosažení cílů organizace. *(Workshop on Capitalism and Socialist Organization – Europian Institute for Advente Studies in Management)*

Management je jevem, který probíhá ve společenských, přírodních i technických systémech a lze ho chápat jako vztah mezi řídícím a řízeným prvkem. Složitost managementu je dána zejména tím, že se jedná o mezilidskou interakci a také tím, že řízeným předmětem jsou složité systémy ve složitých podmínkách. Jeho pět základních

funkcí (technická, obchodní, personální, ekonomická, výrobní) lze chápat jako schopnost realizovat určitý proces.

Čtyři základní prvky (plánování, organizování, stimulování, kontrola) managementu tvoří obecnou řídící činnost, kterou se zajišťuje splnění cílů.
(Němeček, Zich, 2006, 1. díl, s. 11)

- **Plánování** zahrnuje výběr úkolů, cílů a činností potřebných pro jejich dosažení. Plán jako takový pak poskytuje racionální výběr mezi možnostmi budoucího průběhu činností, kdy **cíle** představují budoucí očekávaný stav.
  (Němeček, Zich, 2006, 2. díl, s. 48)
- **Organizování je proces**, který musí zahrnout stanovení cílů firmy, formulování podpůrných cílů, taktik a plánů, identifikaci a klasifikaci činností, potřebných pro jejich dosažení, seskupování těchto činností z hlediska disponibilních lidských materiálních zdrojů tak, aby bylo možné co nejlépe za daných okolností vykonávat, delegování potřebných pravomocí pro vedoucí skupin k provádění daných činností a v neposlední řadě horizontální a vertikální provázání těchto skupin pomocí vztahů nadřízenosti a podřízenosti a pomocí informačních toků. **Organizační strukturu** je třeba pojímat jako organizační podmínku pro dosažení stanovených cílů. Každá organizační struktura by měla být projektována tak, aby bylo jasné, kdo a jaké úkoly má plnit a kdo je odpovědný za výsledky. (Němeček, Zich, 2006, 2. díl, s. 88)
- **Motivace** se v činnosti člověka projevuje jako vnitřní popud působící směrem k vytyčenému cíli. **Stimulace** představuje soubor vnějších incentivů (podnětů, pobídek) usměrňujících jednání pracovníků a působících na jejich motivaci. Smyslem používání stimulů je podnítit u pracovníka určitou aktivitu nebo ji omezit.
  (Němeček, Zich, 2005, s. 15)
- **Kontrola** je zaměřena na měření a kontrolování vykonané práce, aby bylo jisté, že plány budou plněny a cílů dosaženo. Plánování a kontrolování spolu těsně souvisí. Bez cílů a plánů nemůže existovat kontrola, protože vykonaná práce musí být měřena s ohledem na určitá kritéria. Základní **kontrolní proces** zahrnuje stanovení standardů, měření vykonané práce vzhledem ke stanoveným standardům a korekce odchylek od standardů a plánů**. Charakteristické znaky** efektivního kontrolního systému jsou přesnost, včasnost, hospodárnost, flexibilita, srozumitelnost, vhodnost kritérií, strategický rozměr kontroly, ohled na výjimky, několikanásobná kritéria a nápravná opatření. (Němeček, Zich, 2005, s. 23)

2.3.2 Inovační management

- **Definice Evropské unie:**

„Inovace je obnova a rozšíření škály výrobků a služeb a s nimi spojených trhů, vytvoření nových metod výroby, dodávek a distribuce, zavedení změn řízení, organizace práce, pracovních podmínek a kvalifikace pracovní síly.“
(Bartes, 2005, s. 105)

- **Kultura inovace**

Je taková organizace, kde jsou inovace nedílnou součástí, stálou hodnotou a předpokladem pro činnost organizace. Nejedná se o pouhé jednorázové nebo náhodné akce, ale o stálou, trvale udržitelnou inovací. Jež se potom stává součástí kultury korporativní, podnikové. (Bartes, 2005, s. 106)

Inovace a Evropská unie

Předělem v historii Evropské unie se stal mimořádný summit v Lisabonu na jaře 2000, který se zabýval změnou paradigmatu společnosti a stanovil cíl pro další směřování EU: „Státy Evropské unie se stanou do roku 2010 nejkonkurenceschopnější a nejdynamičtější znalostní ekonomikou, založenou na znalostní a inovační společnosti, schopnou udržitelného růstu s více a s lepšími pracovními místy a s více posílenou sociální soudržností.“ V Lisabonu tak byl zahájen proces, který položil důraz na mimo jiné na:

- Konkurence schopnost.
- Informační společnost.
- Sociální kohezi.
- Vytváření evropského prostoru výzkumu a inovací.
- Vytváření příznivého prostředí pro zakládání a rozvoj inovativních podniků, zejména malých a středních. (Bartes, 2005, s. 109-110)

Česká republika se usnesením vlády č. 282 ze dne 19. března 2003 rozhodla, že v rámci Lisabonského procesu bude prosazovat 4 priority, z nichž jedna je **výzkum a vývoj**.

Evropská komise věnuje pozornost kandidátským zemím i v oblasti **podpory inovací** a důrazně doporučuje:

- spolupráci vysokých škol a výzkumných ústavů s průmyslem, zakládání nových technologických orientovaných podniků,
- zakládání vývojových (spin-off) společností,
- podporu regionálních sítí pro podporu spin-off aktivit akademických pracovišť,
- financování inovací – investování tzv. podnikatelských andělů a výcvik investičních analytiků inovačně přátelskou průmyslovou politiku,
- rozvoj všech přímých i nepřímých forem konzultací se zaměstnanci,
- vytváření daňových pobídek, které podpoří dodatečné podnikové investice do inovací. (Bartes, 2005, s. 110)

Inovační systém, infrastruktura a subjekty v České republice

Základní funkcí systému inovačního podnikání v ČR je tvorba a realizace inovační strategie a realizační inovační politiky na vládní i nevládní úrovni. (Bartes, 2005, s. 111)

Inovační sytém tvoří čtyři základní komponenty:

- **řídící složky** – státní a veřejná správa, vláda, ministerstva, regionální a místní správa (legislativní, iniciační a regulační aktivity),
- **vzdělávací systém** – celoživotní učení, zahrnující počáteční a další vzdělávání,
- **finance** – rizikový kapitál (venture capital), rizikové financování (risk funding), předstartovní kapitál (seed capital),
- **inovační podnikání** – firmy a subjekty, které se zabývají inovačními aktivitami v širokém slova smyslu (včetně zahraničních oblastí jako jsou výzkum a vývoj, nové technologie a materiály, rozvoj lidských zdrojů, průzkum a rozvoj trhu, inovační marketing). (Bartes, 2005, s. 112)

Inovační struktura

Systém inovačního podnikání vytvářejí **subjekty**, které jakýmkoliv způsobem participují **v inovačních procesech**. Jsou to zejména:

- orgány státní správy a samosprávy,
- komory,
- banky,
- svazy, agentury, sdružení a nadace,

- pracoviště výzkumu a vývoje,
- zahraniční agentury a organizace,
- podnikatelské subjekty,
- zákazníci, klienti, spotřebitelská veřejnost. (Bartes, 2005, s. 112-113)

Ekonomika – věda – inovace

V ekonomické praxi se dá vysledovat, že **ekonomický vývoj** není plynulý, že jeho vývoje není vždy stálý. Tento jev zkoumal D. Kodratěv, který tvrdil, že každých 50 let dosahuje vrcholu jedna dlouhá technologická vlna. Následně vznikly teorie, které tento cyklus vysvětlují, jako např. Inovační teorie, Kapitálová teorie, Teorie pracovní síly a Teorie demografická a sociálně psychologická.

Mezi autory **teorie inovací** patří zejména J. A. Schumpeter, který je považován za zakladatele moderního pojetí inovací, a který za hnací sílu vlnění hospodářského pohybu považoval právě inovace. Dalším autorem je např. prof. Valenta, který inovaci chápe jako jakoukoliv změnu ve vnitřní struktuře výrobního organismu. Z jeho teorie vychází prof. Vlček, který inovaci považuje za „tvůrčí lidskou aktivitu vyvolávající pozitivní změnu ve struktuře podnikatelských objektů, která má za následek požadovaný a očekávaný pozitivní efekt“.

Sepětí vědy a techniky se uskutečňuje v procesu nazývaném **rozvoj vědy a techniky**, kdy jde o nepřetržitý proces, v němž se poznatky o přírodních a společenských silách materializují v prostředcích , předmětech a metodách.

Při sledování trendu vzájemného vztahu mezi vědeckotechnickým rozvojem a **inovačními procesy** je sledovat trend ke komerčnímu využití výsledků rozvoje vědy a techniky, snahu o zefektivnění výdajů na rozvoj vědy a techniky a růst vědecko výzkumné spolupráce v mezinárodním měřítku. V rámci efektivního řízení je důležitý systém tří pilířů podniku: podniková stabilita, podnikavost a překonávání vžitých stereotypů. (Bartes, 2005)

Inovace znamená změnu, kterou je třeba považovat za normální, zdravý a potřebný jev. Vyhledávání změn však musí být založeno na cílevědomém a organizovaném vyhledávání a jejich systematické analýze. Jedná se o tvůrčí činnost ve veškerých aktivitách podniku, kdy jde o uplatňování neustále nových myšlenek a odpovídajících změn, které se promítají do stylu podnikového chovaní. (Bartes, 2005)

Změny uvnitř oboru (firmy)

Změny, ke kterým dochází uvnitř oboru nebo firmy, může identifikovat ve většině případů pouze odborník – profesionál. K těmto změnám patří: nečekané události, rozpory, potřeby procesu, oborové a tržní struktury. (Bartes, 2005, s. 50)

Změna založená **na rozporu** je ve své podstatě dle Druckera nějaký nesoulad či nesrovnalost mezi tím, co existuje a tím co by mělo existovat, nebo mezi tím co existuje a tím, za co všichni existující jev považují, apod. Tyto nesrovnalosti vytváří nestabilitu, stavy napjatosti apod., které si vynucují nové inovace a mají následující formu rozporu:

- rozpor mez ekonomickými realitami,
- rozpor mezi existující reálnou situací a situací předpokládanou,
- rozpor mezi úsilím vynakládaným v určitém oboru a hodnotami a očekáváním zákazníků,
- vnitřní rozpor v rytmu nebo logice procesu.

Jako základní podmínky pro úspěch při **řešení rozporu** jsou dle Druckera:

- inovační řešení musí být jasně definovatelné,
- musí být proveditelné známou a dostupnou technologií. (Bartes, 2005, s. 53)

Potřeby procesu

Úspěšné inovace založené na potřebách procesu vyžadují splnění následujících kriterií:

- samostatný proces,
- existenci slabého či chybějícího článku (procesu),
- jasnou definici cíle (řešení musí vyhovovat způsob, jakým lidé práci dělají),
- možnost jasně definovat specifikace řešení (nutnost existence znalostí na potřebné řešení),
- obecné uvědomění toho, proč by měl existovat nějaký lepší způsob řešení stávajícího stavu (uživatelé stávajícího procesu musí danou potřebu chápat, nestačí, aby ji pouze pociťovali). (Bartes, 2005, s. 54-55)

Inovační principy:

- analýza příležitostí,
- koncepční a percepční charakter inovace,
- jednoduchost inovace,
- vznik inovace v malém měřítku,
- cílem každé inovace je získání vedoucího postavení na trhu. (Bartes, 2005, s. 60)

Intelektuální kapitál firmy

Podniková intelektuální kapitálová základna má tři základní prvky, a to lidský potenciál, zájmový kapitál a strukturní kapitál.

- **Lidský kapitál** představuje schopnosti, vědomosti, hodnoty a inovační potenciál jednotlivců v dané firmě.
- **Zájmový kapitál** zahrnuje podnikové distribuční a marketingové kanály, síť strategických spojenců a partnerů a loajalitu zákazníků i jejich potenciál podněcovat nové nápady.
- **Strukturní kapitál** (někdy též nazývaný „inovační infrastruktura podniku“). Ve své podstatě zahrnuje podnikový, inovační a vzdělávací potenciál, schopnost týmové práce, strategie, vize, kulturu, informační systémy a nesčetné další nehmotné prvky, které jsou skutečným zdrojem vytváření hodnot a komparativních výhod.
  (Bartes, 2005, s. 62)

2.3.3 Risk management

V nejširším slova smyslu riziko znamená **„vystavení nepříznivým okolnostem“**. Neexistuje jedna, obecně uznávaná, definice rizika, pojem riziko je definován různě:

- pravděpodobnost či možnost vzniku ztráty, obecně nezdaru;
- variabilita možných následků nebo nejistota jejich dosažení;
- odchýlení skutečných a očekávaných výsledků;
- pravděpodobnost jakéhokoli výsledku odlišného od výsledku očekávaného;
- situace, kdy kvantitativní rozsah určitého jevu podléhá jistému rozdělení pravděpodobnosti;
- nebezpečí negativní odchylky od cíle (tzv. čisté riziko;
- nebezpečí chybného rozhodnutí;

- možnost vzniku ztráty nebo zisku (tzv. spekulativní riziko);
- neurčitost spojená s vývojem hodnoty aktiva (tzv.investiční riziko);
- střední hodnota ztrátové funkce;
- možnost, že specifická hrozba využije specifickou zranitelnost systému.
  (Rais, Doskočil, 2007, s. 47)

V ekonomii je pojem riziko užíván v souvislosti s nejednoznačností průběhu určitých skutečných ekonomických procesů a nejednoznačností jejich výsledků; obecně lze samozřejmě konstatovat, že se nemusí jednat pouze o riziko ekonomické. Existují i jiné druhy rizik, např.:

- politická a teritoriální;
- ekonomická – makroekonomická a mikroekonomická, např. tržní, inflační, kursovní, obchodní, platební apod.;
- **bezpečnostní**;
- právní a spojená s odpovědností za škodu;
- předvídatelná a nepředvídatelná;
- specifická – např. pojišťovací, manažerská, finančního trhu, odbytová, inovací apod.
  (Rais, Doskočil, 2007, s. 48)

Analýza rizik

Prvním krokem v procesu snižování rizik je jejich analýza. Analýza rizik je obvykle chápána jako proces definování hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva, tedy stanovení rizik a jejich závažnosti. (Rais, Doskočil, 2007, s. 50)

Analýza rizik zpravidla zahrnuje:

- **identifikaci aktiv** – vymezení posuzovaného subjektu a popis aktiv, které vlastní;
- **stanovení hodnoty aktiv** – určení hodnoty aktiv a jejich význam pro subjekt, ohodnocení možného dopadu jejich ztráty, změny či poškození na existenci či chování subjektu;
- **identifikaci hrozeb a slabin** – určení druhů událostí a akcí, které mohou ovlivnit negativně hodnotu aktiv; určení slabých míst subjektu, které mohou umožnit působení hrozeb;
- **stanovení závažnosti hrozeb a míru zranitelnosti** – určení pravděpodobnosti výskytu hrozby a míry zranitelnosti subjektu vůči dané hrozbě.

Výsledky hodnocení rizik pomohou určit odpovídající kroky vedení organizace i priority pro zvládání rizik a pro realizaci opatření k zamezení jejich výskytu. Je možné, že proces hodnocení rizik a stanovení opatření bude třeba opakovat několikrát, aby byly pokryty různé části subjektu (organizace) nebo jednotlivé činnosti.
(Rais, Doskočil, 2007, s. 51)

Metody analýzy rizik

- **Kvantitativní metody**

Kvantitativní metody jsou založeny na matematickém výpočtu rizika z frekvence výskytu hrozeb a jejího dopadu. Kvantitativní metody jsou více exaktní, než kvalitativní; jejich provedení vyžaduje více času a úsilí.

- **Kvalitativní metody**

Kvalitativní metody se vyznačují tím, že rizika jsou vyjádřena v určitém rozsahu (např. <malé, střední, velké>). Úroveň je určována obvykle kvalifikovaným odhadem. Kvalitativní metody jsou jednodušší a rychlejší, ale i více subjektivní.
Nejběžnější varianta je metoda účelových interview (také **metoda Delphi**), která spočívá na řízeném kontaktu mezi experty hodnotící skupiny a příslušnými představiteli hodnoceného subjektu. Oproti jiným metodám, založených na strojovém zpracování velkého počtu dotazníků, používá metoda Delphi pro rizikovou analýzu souboru otázek diskutovaných na účelových pohovorech přičemž obvykle tyto otázky mají dvě části – pevnou, předem danou, a variabilní, dle průběhu pohovoru a postavení respondenta. Respondenti nepřicházejí do styku při zpracování odpovědí (provádění pohovorů), čímž je zaručeno vzájemné neovlivňování. Výhody této metody jsou: menší náročnost na spotřebu zdrojů a/nebo času, zohlednění specifik posuzovaného informačního systému, jeho správce, okolí, uživatelů apod. Metoda Delphi je vhodná pro analýzu rizik především proto, že určuje, co se může stát za jakých podmínek.
(Rais, Doskočil, 2007, s. 67-69)
Metoda Delphi se do značné míry podobá přístupu prognózování, a to zejména proto, že využívá kolektivní zkušenosti a kolektivního úsudku skupiny expertů. Úspěch či neúspěch metody odvisí na řadě faktorů – např. na vhodném výběru expertů, na kvalitě dotazníků, na jasné, cílevědomé formulaci otázek, na vyhodnocení a rychlém zpracování skupinového názoru na určitý problém. **Cílem metody je zjistit, které změny se mohou uskutečnit a jaké jsou potřeba podmínky k jejich realizaci.**
(Rais, Doskočil, 2007, s. 131)

Management podnikatelských rizik

Management rizik (řízení rizik) je kompletní proces zjištění, kontroly, eliminace a minimalizace nejistých událostí, které mohou ovlivnit subjekt.

Kromě analýzy rizik zpravidla řízení rizik zahrnuje:

- výběr protiopatření,
- analýzu nákladů/přínosů,
- implementaci protiopatření,
- testování (komplexní prověřování) protiopatření. (Rais, Doskočil, 2007, s. 75)

2.3.4 Bezpečnostní politika organizace

Při analýze rizik jede o odhad pravděpodobnosti vzniku každého jednotlivého incidentu a následně pak intenzity jeho následku. Bezpečnostní politika je souhrnem principů a východisek řešení, výchozím bodem pro návrh a realizaci standardů, směrnic, procedur a opatření. Je nutné v ní umět odpovědět na klíčové otázky:

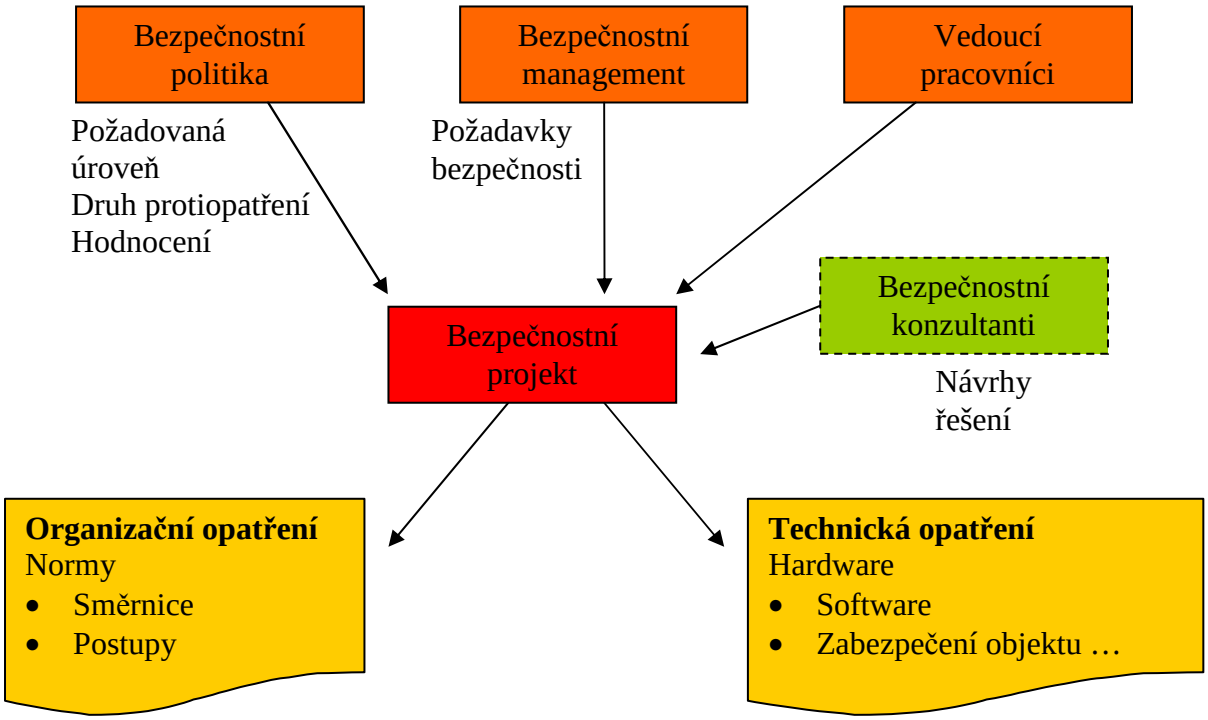
- Co má být chráněno?
- Kdo nese odpovědnost?
- Kdy to bude efektivní?
- Jak to bude vynuceno?
- Kdy a jak to bude realizováno?

Jestliže tedy bezpečnostní politika firmy stanovuje požadovanou úroveň bezpečnosti, navrhuje protiopatření proti rizikům a hodnotí jejich účinnost, pak vlastní bezpečnostní projekt v sobě zahrnuje i požadavky bezpečnostního manažera, vedoucích pracovníků a vede k tvorbě podnikových norem bezpečnosti, směrnic a postupů, společně s technickými opatřeními k snížení rizik. Protože jde zpravidla o velmi specializované činnosti, bývá časté najímání externích bezpečnostních specialistů – konzultantů.

Kromě hlavního manažera odpovědného za bezpečnost je nutné, aby s ním na všech úrovních řízení spolupracovali bezpečnostní specialisté, například v oblasti zabezpečení informačního systému, zabezpečení objektu, dokumentů, a pochopitelně i v oblasti vlastních pracovníků. (Koch, Dovrtěl, 2006, s. 149)

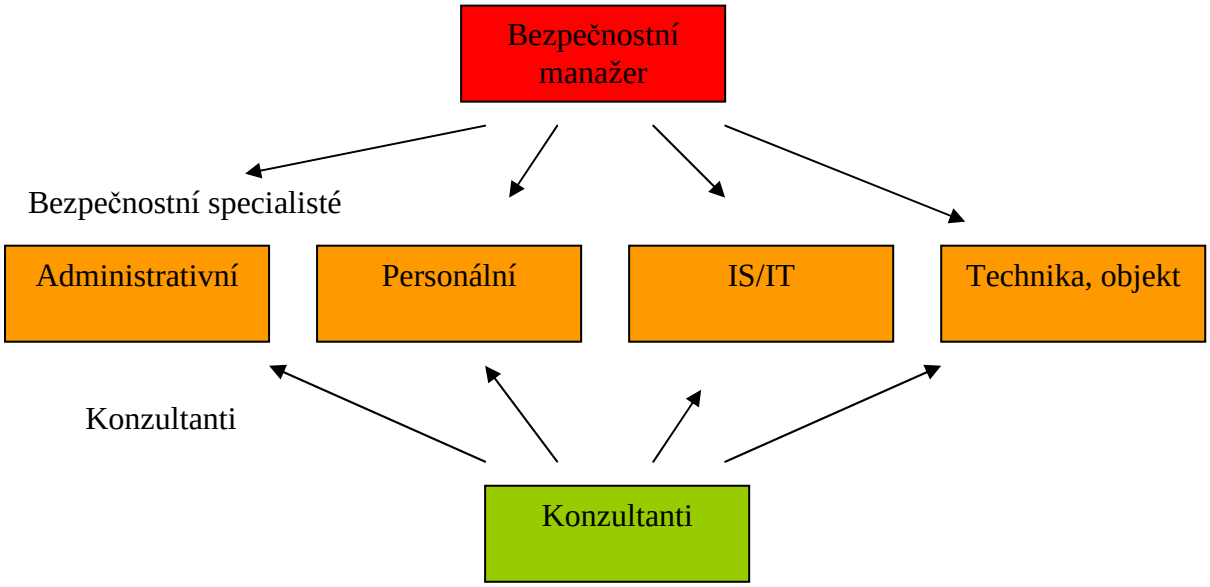
Obrázek č. 1:

Bezpečnostní politika. (Koch, Dovrtěl, 2006, s. 149)



Obrázek č. 2:

Subjekty spolupracující na bezpečnostní politice (Koch, Dovrtěl, 2006, s. 150)



2.4 Osobnost manažera

Na osobnost manažera jsou kladeny vysoké nároky, kdy musí zvládat bezchybně své role v rámci odlišných očekávání svých kolegů, nadřízených nebo podřízených. Požadavky na manažery na různých úrovních řízení jsou odlišné. Důraz je kladen na odbornost manažera, znalosti, schopnosti a dovednosti, stejně jako na jeho osobnostní kvality a osobní zkušenosti.

2.4.1 Evropské standardy manažerské způsobilosti

Evropský institut managementu se sídlem ve Velké Británii má za úkol rozvoj celoevropských standardů manažerské způsobilosti. Standard, který byl tímto institutem zpracován, demonstruje rozsáhlost nároků na manažera, rozdílnosti úloh a z toho plynoucí potřebu znalostí a zkušeností. Pro úroveň středního vedoucího byly stanoveny tyto standardy:

- řídit operace,
- řídit finanční zdroje,
- řídit lidi,
- řídit informace. (Němeček, Zich, 2006, 1. díl, s. 20)

Evropský standard manažerské způsobilosti lze upřesnit:

- iniciovat a zabezpečovat změny a zdokonalení ve službách, výrobcích a systémech,
- sledovat, zabezpečovat a zlepšovat poskytování služeb a výrobků,
- sledovat a řídit užití zdrojů,
- zajišťovat efektivní rozdělení zdrojů na jednotlivé činnosti a projekty,
- podílet se na výběru pracovníků,
- rozvíjet týmy, jednotlivé pracovníky a sebe sama s cílem zvýšit výkon,
- plánovat, rozdělovat a hodnotit práci týmů, jednotlivých pracovníků a sebe sama,
- vytvářet, udržovat a rozvíjet efektivní pracovní vztahy,
- získávat, vyhodnocovat a organizovat relevantní informace,
- zajišťovat informace významné pro řešení problémů a rozhodování.
  (Němeček, Zich, 2006, 1. díl, s. 21)

2.4.2 Manažerská způsobilost v oblasti bezpečnosti

Co by měl znát a prosazovat v oblasti bezpečnosti každý manažer:

- Uvědomit si, že vrcholovou odpovědnost za bezpečnost nese právě on. Pochopit, že podcenění bezpečnostních rizik může vést k ohrožení ekonomické stability organizace nebo narušení kontinuity podnikání, činnosti. Respektovat, že celá řada povinností v bezpečnosti je dána legislativou včetně odpovědnosti vedoucího. Musí bezpečnostní legislativu znát alespoň rámcově, včetně rizika uložených sankcí.
- Ztotožnit se s tím, že bezpečné chování organizace je velmi úzce spojeno s jeho vlastní bezpečnostní a naopak. Chovat se bezpečně. Osobně znát a dodržovat požadavky bezpečnostní legislativy, zejména ve vztahu k ochraně osob a informací. Využít nabídky pro vzdělání se v této oblasti. Naučit se nakládat s bezpečnostními informacemi jako s financemi. Dodržovat zásadu „need to know“ pro veškerou práci s kvalifikovanými a dalšími citlivými informacemi. Nezveřejňovat zdroje získaných bezpečnostních informací.
- Za klíčovou osobu pro řešení komplexní bezpečnosti považovat bezpečnostního manažera. Zajistit mu odpovídající postavení v organizační struktuře a vybavit ho nezbytnými pravomocemi. Obracet se na něho při řešení všech bezpečnostních problémů. Kontakt s bezpečnostním manažerem má být přímý. Čím dále je vrcholový manažer od bezpečnosti, tím více je vystaven bezpečnostním rizikům. Vedení musí být o stavu bezpečnosti periodicky informováno. Jeden bezpečnostní manažer může zajišťovat služby i pro několik organizací.
- Řízení bezpečnosti se musí odehrávat systémově a komplexně. Základem řízení bezpečnosti je bezpečnostní politika, která byla vytvořena na základě analýzy rizik. Rozpočet na bezpečnost by měl být samostatnou kapitolou financování. Zpracování bezpečnostní politiky a další řídící dokumentace v této oblasti je možno zajistit dodavatelsky. Dodavatel těchto služeb by neměl být současně jejich realizátorem.
- Vyžadovat u všech podřízených prosazování a hodnocení bezpečnosti jako součást procesu řízení.
- Bezpečnost není jenom o nejnižší ceně dodávek outsourcovaných služeb, důležitými kriterií jsou kvalita a spolehlivost. Cena by proto neměla být jediným měřítkem. Pokud si nejste kvalitou služeb jisti, zadejte odborné posouzení

specializované firmě, nezávislému expertovi či soudnímu znalci. Kvalitní konzultační služby je nutné zajistit i v tomto oboru.

- Bezpečnost vyžaduje jako ostatní oblasti periodickou údržbu a kontrolu. Manažera by proto neměly výstupy auditů a kontrol bezpečnosti zajímat jen tehdy, když se stane mimořádná událost. Pro ověření efektivnosti bezpečnostních opatření, kvality outsourcových služeb a optimalizace nákladů má využívat externí bezpečnostní audit. Dodavatelem auditu nemají být z důvodu objektivnosti posouzení dodavatelé bezpečnostních technologií ani bezpečnostní služby.
- Znát rámcově činnosti, které zajišťuje bezpečnostní manažer (útvar). Jedná se o ochranu osob včetně VIP a bezpečnostního vzdělání. Ochrana hmotného majetku. Ochrana kvalifikovaných a důležitých informací BOZP a požární ochrana. Bezpečnost informačních a komunikačních technologií. Řešení mimořádných událostí a bezpečnostních incidentů. Krizové řízení a business kontinuita. Komerční obranné zpravodajství. Zajišťování spolupráce s bezpečnostními složkami a orgány činnými v trestním řízení. Technologická bezpečnost a havarijní plány. Řízení výkonu a kvality outsourcových služeb (Quality Monitoring). Vydávaní interních předpisů v oblasti bezpečnosti a kontroly bezpečnosti. (Fryšar a kol., 2006)

3 Analýza problému a současná situace

3.1 Metodika

Vzhledem k tomu, že zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů (dále také „Zákon“) definuje povinnosti při ochraně osobních údajů (dále také „OOÚ“), ale ponechává volnost v tom, jak tyto povinnosti naplnit, bylo nutné nejdříve stanovit metodiku, kterou budu při zpracování diplomové práce postupovat. Protože neexistuje žádný standard, který by se ochranou osobních údajů výslovně zabýval, orientovala jsem se na standardy, které řeší obecně bezpečnost informací. Při výběru vhodného standardu jsem vycházela z faktu, že osobní údaje jsou informacemi a musí se chránit stejnými prostředky jako každá jiná informace.

Pro řešení problematiky bezpečnosti informací je nejrozšířenější používání standardů ISMS. Standard ČSN ISO/IEC 17799 Informační technologie – Bezpečnostní techniky – Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací (dále také „standard“) vznikl jako praktická sbírka nejlepších praktik ("best practices") v oboru bezpečnosti informací a na jejím vzniku se podílela řada státních subjektů ve spolupráci s komerčními organizacemi. Tento standard ale pouze popisuje doporučené postupy.

Druhý ze standardů ISMS je ČSN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky, jenž stanoví požadavky pro aplikaci standardu ČSN ISO/IEC 17799 v organizaci. Standard ČSN ISO/IEC 27001 obsahuje přílohu „A“, ve které je shrnut přehled všech bezpečnostních cílů a opatření, které jsou podrobněji popsány v ČSN ISO/IEC 17799. Tato příloha představuje jakousi „mapu“ všech možných bezpečnostních opatření, které lze pro organizaci použít. (Ve standardu je ve statích 5 až 15 definováno 11 oblastí bezpečnosti, 39 cílů a 133 bezpečnostních opatření pro zajištění bezpečnosti informací v organizaci).

Vzhledem k faktu, že tento standard řeší komplexně problematiku bezpečnosti informací u organizace, zatímco Zákon pokrývá jen část této problematiky, použila jsem pro hodnocení jenom ty oblasti bezpečnosti a cíle, které mají významnou relevanci k problematice Zákona. Vlastní posouzení stávajícího stavu OOÚ bylo rozděleno podle takto vybraných oblastí a jejich hodnocení provedeno metodou Delphi. Tato metoda

využívá kolektivní zkušenosti a úsudku skupiny expertů; v případě této diplomové práce se jednalo o vedoucí zaměstnance odpovědné za jednotlivé úseky činností státního zastupitelství. Prostudováním příslušné dokumentace a následně prováděnými pohovory s jednotlivými vedoucími, jsem zjišťovala stávající stav ve zpracovávané problematice. S každým odpovědným pracovníkem jsem hovořila samostatně, abych omezila jistou míru možného ovlivnění. Mým cílem bylo pomocí uvedené metody zjistit, které změny se mohou uskutečnit a jaké podmínky jsou třeba k jejich realizaci.

3.1.1 Vymezení oblastí a cílů bezpečnosti

V této kapitole diplomové práce byly zpracovány jednotlivé oblasti a cíle bezpečnosti, které vycházejí ze Standardu:

- **Bezpečnostní politika**

Bezpečnostní politika informací

Cíl: Definovat směr a vyjádřit podporu bezpečnosti informaci ze strany vedení v souladu s požadavky organice, příslušnými zákony a regulatorními požadavky.

- **Organizace bezpečnosti**

Interní organizace

Cíl: Řídit bezpečnost informací v organizaci.

Externí subjekty

Cíl: Zachovat bezpečnost informací organizace a prostředků pro zpracování informací, které jsou přístupné, zpracovávané, sdělované nebo spravované externími subjekty.

- **Klasifikace a řízení aktiv**

Odpovědnost za aktiva

Cíl: Udržovat přiměřenou ochranu aktiv organizace

- **Bezpečnost lidských zdrojů**

Před vznikem pracovního vztahu

Cíl: Zajistit, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybráni vhodní kandidáti a snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace.

Během pracovního vztahu

Cíl: Zajistit, aby si zaměstnanci, smluvní a třetí strany byli vědomi bezpečnostních hrozeb a problémů s nimi spjatých, svých odpovědností a povinností a byli připraveni podílet se na dodržování politiky bezpečnosti informací během své běžné práce a na snižování rizika lidské chyby.

Ukončení nebo změna pracovního vztahu

Cíl: Zajistit, aby ukončení nebo změna pracovního vztahu zaměstnanců, smluvních a třetích stran proběhla řádným způsobem.

- **Fyzická bezpečnost a bezpečnost prostředí**

Zabezpečené oblastí

Cíl: Předcházet neautorizovanému přístupu do vymezených prostor, předcházet poškození a zásahům do provozních budov a informací organizace.

Bezpečnost zařízení

Cíl: Předcházet ztrátě, poškození nebo kompromitaci aktiva přerušení činnosti organizace.

- **Řízení komunikací a řízení provozu**

Provozní postupy a odpovědnosti

Cíl: Zajistit správný a bezpečný provoz prostředků pro zpracování informací.

Plánování a přejímání informačních systémů

Cíl: Minimalizovat riziko selhání informačních systémů.

Ochrana proti škodlivým programům a mobilním kódům

Cíl: Chránit integritu programů a dat.

Zálohování

Cíl: Udržovat integritu a dostupnost informací a prostředků pro jejich zpracování.

Bezpečnost při zacházení s médii

Cíl: Udržovat integritu a dostupnost informací a prostředků pro jejich zpracování.

Výměny informací

Cíl: Zajistit bezpečnost informací a programů při jejich výměně v rámci organizace a při jejich výměně s externími subjekty.

Monitorováni

Cíl: Detekovat neoprávněné zpracování informací.

- **Řízení přístupu**

Požadavky na řízení přístupu

Cíl: Řídit přístup k informacím.

Řízení přístupu uživatelů

Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k informačním systémům.

Odpovědnosti uživatelů

Cíl: Předcházet neoprávněnému uživatelskému přístupu, prozrazení nebo krádeži informací a prostředků pro zpracování informací.

Řízení přístupu k síti

Cíl: Předcházet neautorizovanému přístupu k síťovým službám.

Řízení přístupu k operačnímu systému

Cíl: Předcházet neautorizovanému přístupu k operačním systémům.

Řízení přístupu k aplikacím a informacím

Cíl: Předcházet neoprávněnému přístupu k informacím uloženým v počítačových systémech.

Mobilní výpočetní zařízení a práce na dálku

Cíl: Zajistit bezpečnost informací při použití mobilní výpočetní techniky a při využití zařízení pro práci na dálku.

- **Zvládání bezpečnostních incidentů**

Hlášení bezpečnostních událostí a slabin

Cíl: Zajistit nahlášení bezpečnostních událostí a slabin informačního systému způsobem, který umožní včasné zahájení kroků vedoucích k nápravě.

Zvládáni bezpečnostních incidentů a kroky k nápravě

Cíl: Zajistit odpovídající a účinný přístup ke zvládání bezpečnostních incidentů.

- **Soulad s požadavky**

Soulad s právními normami

Cíl: Vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.

Soulad s bezpečnostními politikami, normami a technická shoda

Cíl: Zajistit shodu systémů s bezpečnostními politikami organizace a normami.

Hlediska auditu informačních systémů

Cíl: Maximalizovat účinnost auditu a minimalizovat zásahy do informačních systémů.

3.1.2 Definování požadavků § 13 Zákona

Pro posuzování současného stavu opatření podle § 13 Zákona, jsou uvedeny požadavky v něm stanovené:

- **odst. 1)** Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.

- **odst. 2)** Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.

- **odst. 3)** V rámci opatření podle odstavce 1 správce nebo zpracovatel posuzuje rizika týkající se:
  a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům,
  b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,
  c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje,
  d) opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

- **odst. 4)** V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel v rámci opatření podle odstavce 1 povinen také:
  a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,
  b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,
  c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány,
  d) zabránit neoprávněnému přístupu k datovým nosičům.

3.2 Posouzení současného stavu přijatých opatření

Ve své diplomové práci jsem provedla posouzení současného stavu přijatých opatření k ochraně osobních údajů u okresního státního zastupitelství (dále také „OSZ“), které spadá do obvodu působnosti Krajského státního zastupitelství v Brně.

Při posuzování jsem postupovala podle oblastí uvedených v předchozí kapitole 3.1.1, kdy cíle slouží pouze pro logické uspořádání, resp. logickou kategorizaci oblastí bezpečnosti, a protože se však jedná o rozsáhlý počet celků, je pro lepší přehlednost za každým popsaným stávajícím stavem uveden tzv. „požadavek“. Tento požadavek je určitým návodem k realizaci stavu, který by měl být v organizaci zaveden. Celkové vyhodnocení analýzy je shrnuto v kapitole 3.4 nazvané Výsledky analýzy, souhrn nejzávažnějších nedostatků.

3.2.1 Bezpečnostní politika

Cíl: *Definovat směr a vyjádřit podporu bezpečnosti informaci ze strany vedení v souladu s požadavky organizace, příslušnými zákony a regulatorními požadavky.*

V rámci okresního státního zastupitelství **není bezpečnostní politika definována**. Obecná pravidla jsou nepřímo popsaná v dokumentech Kancelářský řád, Organizační řád a dalších interních předpisech, neexistuje však dokument, který by zastřešoval principy řízení bezpečnosti.

Požadavek: *Dokument bezpečnostní politiky informací by měl být schválen vedením organizace, vydán a být dán na vědomí všem zaměstnancům a relevantním třetím stranám. Bezpečností politika by měla být vrcholovým a sjednocujícím dokumentem, který shrne veškeré hlavní bezpečnostní zásady a bude zdrojem odkazů na ostatní dokumenty.*

- Současný stav řízení bezpečnosti informací je takový, že bezpečnostní zásady a požadavky jsou formulovány v různých dokumentech, a to:

- Pokyn obecné povahy nejvyššího státního zástupce, kterým se vydává **Kancelářský řád státního zastupitelství** (dále také Kancelářský řád), v tomto dokumentu je řešena výhradně administrativní bezpečnost,
- Instrukce ministerstva spravedlnosti, kterou se vydává **Skartační řád státního zastupitelství** (dále také Skartační řád),
- Organizační opatření krajského státního zástupce o **Provozním řádu počítačových sítí** v působnosti Krajského státního zastupitelství v Brně (dále také Provozní řád počítačových sítí),
- Organizační opatření jímž se vydává **Ukládací řád agend vedených na počítačích** u okresního státního zastupitelství (dále také OSZ), který zejména definuje osobní odpovědnosti za archivaci a zálohování údajů (dále také Ukládací řád) a který je pravidelně 1x za rok aktualizován,
- Organizační opatření KSZ, kterým se vydává **Pracovní řád Krajského státního zastupitelství v Brně a státních zastupitelstvích v jeho působnosti** (dále jen Pracovní řád), které je závazné i pro OSZ,
- **Organizační řád** okresního státního zastupitelství popisuje organizaci práce, stanovuje úkoly, povinnosti a odpovědnosti jednotlivých zaměstnanců OSZ, včetně odpovědnosti za vybrané kategorie informací (dále také Organizační řád) a který je pravidelně aktualizován,
- **Organizační opatření OSZ**, kterým se stanoví zásady bezpečnosti a ostrahy v budově OSZ, a kterým se vydává návštěvní řád, ale který **neobsahuje stanovení** pravidel pro přijímání návštěv,
- **Organizační opatření OSZ**, kterým se vydává zmocnění pro kontrolu výkonu justiční stráže bezpečnostnímu řediteli.

- Bezpečnostní zásady prosazované u okresního státního zastupitelství jsou uvedeny ve všech výše uvedených dokumentech.

Požadavek: *Bylo by vhodné dopracovat Návštěvní řád s pravidly pro přijímání návštěv, která nejsou popsána v žádném z výše uvedených dokumentů.*

- Přezkoumání a aktualizace bezpečnostní politiky **není prováděna**, protože bezpečnostní politika nebyla formulována. Tím je způsobeno, že jakákoli změna

v přístupu k řešení bezpečnosti musí být promítána do jednotlivých dokumentů, což má za následek větší pravděpodobnost opomenutí promítnutí požadované změny ve všech dokumentech, kterých se problematika bezpečnosti týká. Řídící dokumenty **jsou ale pravidelně aktualizovány**.

Požadavek: *Pro zajištění její neustálé použitelnosti a účinnosti by bezpečnostní politika informací měla být přezkoumávána v plánovaných intervalech a vždy, když nastane významná změna.*

- Plán kontrolní činnosti je řešen pouze na úrovni KSZ a to zejména směrem k oblasti personální práce a spisové služby.

Požadavek: *Bylo by vhodné zpracovat, případně rozšířit vlastní plán úkolů o kontrolní činnost vůči jednotlivým oblastem ochrany osobních údajů, a to zejména oblasti fyzické, personální a administrativní bezpečnosti.*

- Oblast počítačové bezpečnosti (automatizované zpracování osobních údajů) je řešena z úrovně krajského státního zastupitelství a částečně i vlastními opatřeními z úrovně OSZ, které jsou uvedeny výše.

3.2.2 Organizace bezpečnosti

- **Interní organizace**

Cíl: *Řídit bezpečnost informací v organizaci.*

Závazek vedení a koordinace bezpečnosti informací

Požadavek: *Vedení organizace by mělo stanovit jasný směr a aktivně podporovat bezpečnost v rámci organizace. Mělo by demonstrovat svůj závazek a jednoznačně přiřadit a vymezit role v oblasti bezpečnosti informací.*

Předpokladem reálného prosazení bezpečnosti do kterékoli organizace je to, aby vedení organizace vyžadovalo dodržování požadavků na bezpečnost od zaměstnanců a také aby vytvořilo odpovídající podmínky pro zajištění bezpečnosti. Pro prosazení bezpečnosti by bylo vhodné na úrovni OSZ vymezit odpovědnosti za bezpečnost informací a stanovit procesy, kterými bude bezpečnost zajišťována.

- V současnosti tento závazek vychází z dokumentu Kancelářský řád a částečně z dokumentu Organizační řád.

Přidělení odpovědností v oblasti bezpečnosti informací

Požadavek: *Měly by být jednoznačně určeny odpovědnosti v oblasti bezpečnosti informací.*

- Přidělení odpovědnosti v oblasti bezpečnosti informací je řešeno v ustanoveních Kancelářského řádu a Provozního řádu počítačových sítí. Jde o organizační zajištění chodu kancelářské služby, rozsah a způsob vedení počítačové evidence, ochrana dat a nahlížení do spisů a zapůjčování spisů. Částečně se také přidělení odpovědností promítá v Organizačním řádu, kde jsou stanoveny odpovědnosti státních zástupců, vedoucí správy, bezpečnostního ředitele, vedoucí kanceláří a pracovníků pověřených vedením rejstříků.
- Explicitně **není ustanovena** osoba, která by řídila a koordinovala bezpečnost informací. Touto osobou by mohl být bezpečnostní ředitel, který by měl kompetence stanovené v rámci celého okresního státního zastupitelství.

Schvalovací proces prostředků pro zpracování informací

Požadavek: *Měl by být ustaven a zaveden postup schvalování (vedoucími zaměstnanci) nových prostředků pro zpracování informací.*

- Bezpečnostní schvalování nasazení nových prostředků pro zpracování informací je zavedeno. Provádí se pouze evidence zařízení. Většina zařízení je pořizována centrálně z nadřízených subjektů organizace, o takto přidělených zařízeních není dodán záznam o schválení k provozu (vyhovující bezpečnostním požadavkům kladených na systém, ve kterém budou provozovány). Tento záznam zůstává založen u nadřízeného státního zastupitelství.

Dohody o ochraně důvěrných informací

Požadavek: *Měly by být určeny a v pravidelných intervalech přezkoumávány dohody obsahující požadavky na ochranu důvěrnosti nebo povinnost zachovávat mlčenlivost, reflektující potřeby organizace na ochranu informací.*

- Požadavek mlčenlivosti je definován v Pracovním řádu (povinnosti zaměstnanců), stejně tak je zde stanovena jeho závaznost pro zaměstnance a zaměstnavatele.

- V pracovní smlouvě, založené v osobním spisu každého zaměstnance, je ustanovení, kterým se zaměstnanec „zavazuje zachovávat mlčenlivost o všech skutečnostech, o nichž se dozvěděl při výkonu zaměstnání a které v zájmu zaměstnavatele nelze sdělovat jiným osobám, pokud této povinnosti nebude v souladu se zákonem zproštěn. Současně bere na vědomí, že porušení této povinnosti je zvlášť hrubým porušením pracovní kázně a je důvodem pro okamžité zrušení pracovního poměru“.
- U pracovních smluv, uzavřených v posledních letech, se zaměstnanec zavazuje zachovávat mlčenlivost i po ukončení pracovního poměru.

Nezávislá přezkoumání bezpečnosti informací

Požadavek: *Přístup organizace k řízení a implementaci bezpečnosti informací (tj. cíle opatření, jednotlivá opatření, politiky, směrnice a postupy) by měly být v pravidelných intervalech (nebo v případě jakékoliv významné změny ve vztahu k bezpečnosti) nezávisle přezkoumávány.*

- Nezávislé přezkoumání bezpečnosti informací nebylo zatím realizováno, ale lze říct, že vedení státního zastupitelství si je vědomo jeho důležitosti pro zajištění toho, zda je přístup k řízení bezpečnosti informací vyhovující, přiměřený a dostatečně účinný.
- Jsou pravidelně prováděny dohledové prověrky z nadřízeného stupně (KSZ) na vybrané kategorie činností, s periodou jedenkrát ročně.
- Pravidelné nezávislé přezkoumávání bezpečnosti se provádí jen v souvislosti s ochranou utajovaných informací, v rozsahu požadavků zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti.

- **Externí subjekty**

Cíl: *Zachovat bezpečnost informací organizace a prostředků pro zpracování informací, které jsou přístupné, zpracovávané, sdělované nebo spravované externími subjekty.*

Identifikace rizik plynoucích z přístupu externích subjektů

Požadavek: *Předtím, než je externím subjektům povolen přístup k informacím organizace a prostředkům pro zpracování informací, by měla být identifikována rizika a zavedena vhodná opatření na jejich pokrytí.*

Informace mohou být ohroženy přístupem třetích stran s neadekvátním řízením bezpečnosti. Je nutné vědět, jaká opatření je nezbytné přijmout v souvislosti se zabezpečením přístupu třetích stran k prostředkům pro zpracování informací.

- Návštěvní řád je písemně stanoven, ale režim návštěv je přizpůsoben osvědčeným zvykovým pravidlům, u kterých ale neplatí princip vymahatelnosti při jejich porušení. **Není písemně stanoven** režim vstupu a přijímání návštěv v písemné podobě, závazný pro všechny zaměstnance OSZ.
- Pravidlo „čistého stolu“ není dodržováno a **není** nikde formálně zakotveno a popsáno.
- Trestní oznámení se v písemné podobě podává na podatelně OSZ. Ústní trestní oznámení se podává ve výslechové místnosti za přítomnosti pověřeného státního zástupce a zapisovatelky.
- Úklid kanceláří (vyjma zabezpečené oblasti ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti a místnosti se servery) a ostatních prostor OSZ je prováděn vlastními zaměstnanci, částečně v pracovní době, částečně po pracovní době (v režimu od 12,00 – 20,00 hod.). Platí pravidlo, že kanceláře se uklízí **zásadně** po pracovní době, **vždy bez přítomnosti daného vlastníka aktiv** (kanceláře). Zaměstnanec provádějící úklid, má podepsaný závazek o mlčenlivosti a je poučen. Přesto zde vzniká značné riziko neoprávněného přístupu k osobním údajům a jiným citlivým informacím, vzhledem k obvyklé a zažité nepřítomnosti vlastníka kanceláře při úklidu.
- Dalšími externími subjekty mohou být praktikanti (stážisté). Na úrovni OSZ jsou praktikanti v rámci praxe poučeni o povinnosti zachovávat mlčenlivost o všech věcech, o kterých se dozvěděli při výkonu své činnosti. Poučení se týká i seznámení s hlavními řídícími předpisy a je stvrzeno podpisem praktikanta. Zakládá se u vedoucí správy OSZ.

- Dozorové spisy jsou uloženy v kancelářích rejstříků ve skříních a volně přístupných vitrínách, mohou být ale uloženy i v kancelářích státních zástupců v uzamykatelných skříních. Klíče od skříní jsou ale obvykle ponechávány v zámcích. Tím vzniká značné riziko neoprávněné manipulace s osobními údaji zejména při provádění úklidu a přijímání návštěv, včetně pracovních.
- Správní spisy a osobní spisy jsou uloženy u vedoucí správy. Všechny spisy obsahující osobní údaje jsou v uzamykatelných skříních.
- Uzavřené dozorové i správní spisy jsou uloženy na dvou spisovnách OSZ, které jsou uzamčeny a zabezpečeny elektrickou zabezpečovací signalizací. Za spisovny odpovídá samostatná administrativní pracovnice, kterou zastupuje v její nepřítomnosti pověřená kolegyně. Pro ukládání starších spisů je využívána spisovna v budově okresního soudu. Klíče od této spisovny si přebírá určená pracovnice od správce budovy okresního soudu. Dále je zřízena tzv. „pomocná spisovna“ s mladšími (ostatními) uzavřenými spisy v prostorách OSZ, která je volně přístupná všem pracovníkům administrativy.
- Kopírovací zařízení jsou v kancelářích jednotlivých pracovníků a síťová tiskárna je ve speciální místnosti.

Bezpečnostní požadavky pro přístup klientů

Požadavek: *Předtím, než je klientům umožněn přístup k informacím a aktivům organizace by měly být zjištěny veškeré požadavky na bezpečnost.*

- Povolování přístupu je zakotveno v Organizační řádu okresního státního zastupitelství.
- Dozorové spisy v listinné podobě jsou přístupné státnímu zástupci, který věc trestní řeší a příslušnému pracovníku administrativy OSZ. Ke správním spisům má přístup pouze vedoucí správy, ostatní pracovníci jen při vyžádání. Toto neplatí pro přístup k osobním spisům zaměstnanců. Zde platí pravidlo, že mohou nahlížet pouze nadřízení do spisů podřízených. Oběh spisů je vyznačen.
- Osobní údaje se také nacházejí v aplikaci ISYZ (elektronické rejstříky trestních spisů), kdy přidělování přístupových oprávnění provádí vedoucí správy, která je správcem aplikace. Postup je formálně popsán a zakotven v Organizačního řádu. Přístupové oprávnění není možné přidělit třetí straně, vyjma pracovníkům KSZ v rámci kontrolní činnosti, s právem pouhého čtení. Vedoucí správy přidělí uživatelské jméno a první přístupové heslo, které si uživatel následně změní. Vede

evidenci prvních přidělených přístupových hesel a následně provádí kontrolu jejich změny. Vedoucí správy je schopna definovat seznam přístupů k jednotlivým rejstříkům v aplikaci ISYZ. V případě zastupování proces zabezpečuje vedoucí kanceláře, která má stejná oprávnění jako vedoucí správy (správce aplikace). Má své vlastní uživatelské jméno a heslo, takže přístup do systému je zpětně kontrolovatelný. Zastupitelnosti vedoucí správy je řešen opět v Organizačním řádu.

3.2.3 Klasifikace a řízení aktiv

- **Odpovědnost za aktiva**

Cíl: *Zajištění přiměřenosti ochrany informačních aktiv.*

Evidence aktiv

Požadavek: *Měla by být identifikována všechna aktiva organizace, všechna důležitá aktiva by měla být evidována a seznam udržován aktuální.*

Evidence by měla obsahovat informace potřebné pro případ obnovy po havárii. Měl by být uveden typ aktiva, jeho formát, umístění, informace o záloze, licenční informace a jeho hodnota pro organizaci.

- Listinná aktiva se evidují v systému ISYZ. Kancelářský řád dává podrobný návod jak evidovat listinná aktiva.
- V oblasti problematiky informačních technologií (dále také IT) je evidence aktiv řešena na úrovni fyzických aktiv (inventurního seznamu materiálu).
- Informační aktiva jsou také podchycena z hlediska evidence databází. Evidence obsahuje informace potřebné pro případ obnovy po havárii. Obsahuje typ aktiva, jeho formát, umístění, informace o záloze, licenční informace a jeho hodnotu pro organizaci. Problematika je řešena v Ukládacím řádu, včetně stanovení odpovědností za zálohování a archivaci.

Přípustné použití aktiv

Požadavek: *Měla by být ustavena, zdokumentována a do praxe zavedena pravidla pro přípustné použití informací a aktiv souvisejících s prostředky pro zpracování informací.*

- U OSZ je v oblasti listinných dokumentů aplikovatelný Kancelářský řád. V oblasti IT definuje požadavky na přípustné použití aktiv Provozní řád počítačových sítí.

Bezpečnostní požadavky na ochranu osobních údajů v osobních spisech popisuje Instrukce Ministerstva spravedlnosti ČR, kterou se stanoví způsob vedení osobního spisu.

3.2.4 Bezpečnost lidských zdrojů

- **Před vznikem pracovního vztahu**

Cíl: *Zajistit, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybráni vhodní kandidáti a snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace.*

Role a odpovědnosti

Požadavek: *Role a odpovědnosti zaměstnanců, smluvních a třetích stran v oblasti bezpečnosti informací by měly být stanoveny a zdokumentovány v souladu s bezpečnostní politikou organizace.*

- Role a odpovědnosti zaměstnanců z hlediska ochrany osobních údajů nejsou z hlediska bezpečnosti v oblasti lidských zdrojů definovány, ale lze na tuto problematiku použít v oblasti listinných dokumentů ustanovení Kancelářského řádu a na oblast IT lze obecně aplikovat požadavky Provozního řádu počítačových sítí. I zde se projevuje chybějící bezpečnostní politika. Současně lze pro oblast listinného i automatizovaného zpracování osobních údajů využít rolí a odpovědností stanovených v organizačním řádu, kde jsou přiděleny zejména odpovědnosti k vedeným rejstříkům.

Podmínky výkonu pracovní činnosti

Požadavek: *Pracovní smlouvy uzavřené se zaměstnanci, smluvními a třetími stranami by měly obsahovat ustanovení o jejich odpovědnostech za bezpečnost informací.*

- Závazek mlčenlivosti o veškerých informacích je zakotven v pracovní smlouvě, uložené v osobním spisu.

- **Během pracovního vztahu**

Cíl: *Zajistit, aby si zaměstnanci, smluvní a třetí strany byli vědomi bezpečnostních hrozeb a problémů s nimi spjatých, svých odpovědností a povinností a byli připraveni podílet se na dodržování politiky bezpečnosti informací během své běžné práce a na snižování rizika lidské chyby.*

Povědomí, vzdělávání a školení v oblasti bezpečnosti informací

Požadavek: *Všichni zaměstnanci organizace, a je-li to důležité i pracovníci smluvních a třetích stran, by měli s ohledem na svoji pracovní náplň, projít odpovídajícím a pravidelně se opakujícím školením v oblasti bezpečnosti informací, bezpečnostní politiky a směrnicím organizace.*

- Problematika školení je řešena pouze obecně v Pracovním řádu v § 33, který ale nezmiňuje ani bezpečnost informací ani školení v používání prostředků výpočetní techniky. Školení je nejdůležitějším prostředkem pro zvyšování bezpečnostního povědomí zaměstnanců organizace. **Neexistence soustavného systému školení** pracovníků OSZ je **závažným nedostatkem** v zajišťování bezpečnosti informací.
- Pravidelné školení v periodě 1x ročně je prováděno pouze ve vztahu k zákonu č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

- **Ukončení nebo změna pracovního vztahu**

Cíl: *Zajistit, aby ukončení nebo změna pracovního vztahu zaměstnanců, smluvních a třetích stran proběhla řádným způsobem.*

Odpovědnosti za ukončení pracovního vztahu

Požadavek: *Měly by být jasně definovány a přiděleny odpovědnosti pro případ ukončení nebo změny pracovního vztahu.*

- Problematika je řešena v Pracovním řádu. Organizování ukončení pracovního vztahu je řešeno s upozorněním na dodržení mlčenlivosti a důrazem na vrácení materiálu.
- V oblasti IT je problematika řešena na základě popsaného postupu, založeného na principu osobní odpovědnosti vedoucí správy z úrovně správce aplikace. Na úrovni správce systému ruší přístupová oprávnění administrátor, a to na základě písemné informace personálního oddělení. Proces rušení je popsán v Organizačním řádu a

částečně v Provozním řádu počítačových sítí. O provedeném zrušení uživatelského účtu je následně proveden písemný záznam.

- U pracovních smluv, uzavřených v posledních letech, se zaměstnanec zavazuje zachovávat mlčenlivost i po ukončení pracovního poměru.

Požadavek: *Při ukončení pracovního vztahu by měli zaměstnanci, pracovníci smluvních a třetích stran odevzdat veškeré jim svěřené předměty, které jsou majetkem organizace.*

- Realizuje se prostřednictvím tzv. „kolečka“, kdy zaměstnancům potvrdí jednotliví správci materiálu vrácení všech zapůjčených předmětů. Povinnost vrátit všechny předměty je zakotvena v Pracovním řádu.

Odebrání přístupových práv

Požadavek: *Při ukončení pracovního vztahu by měla být uživatelům, smluvním a třetím stranám odejmuta nebo pozměněna přístupová práva k informacím a prostředkům pro zpracování informací.*

- Problematika je popsána do Organizačního řádu a částečně v Provozním řádu počítačových sítí. Odebírání přístupových práv realizuje vedoucí správy.

3.2.5 Fyzická bezpečnost a bezpečnost prostředí

➢ **Zabezpečené oblasti**

Cíl: *Předcházet neautorizovanému přístupu do vymezených prostor, předcházet poškození a zásahům do provozních budov a informací organizace.*

Fyzický bezpečnostní perimetr

Požadavek: *Při ochraně prostor, ve kterých se nachází informace nebo prostředky pro zpracování informací, by měly být používány bezpečnostní perimetry (bariéry jako například zdi, vstupní turniket na karty nebo recepce).*

- Perimetr budovy je řádně zabezpečen a střežen justiční stráží v režimu zahájení jednu hodinu před a ukončení jednu hodinu po pracovní době, stanovené Pracovním řádem. V mimopracovní době je objekt napojen na Pult centralizované ochrany Policie ČR (dále také „PCO PČR“).

- V budově se nachází zabezpečená oblast podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, proto má OZS zpracován i projekt fyzické bezpečnosti (dále také „PFB“) a tomu odpovídá i režim vstupu do prostor OSZ.
- OSZ je zabezpečeno systémem elektrické zabezpečovací signalizace (dále také „EZS“), kde výstupy poplachových stavů jsou vyvedeny na stanoviště justiční stráže a současně na PCO PČR. Přístupová oprávnění k aktivaci a deaktivaci systému EZS mají všichni zaměstnanci OSZ a příslušníci justiční stráže (včetně pracovnice určené pro úklid), vyjma přístupu do zabezpečené oblasti. Určené osoby OSZ, definované v PFB, vlastní přístupová oprávnění, která lze využít pro přístup do zabezpečené oblasti. Seznam těchto osob a jejich přístupových oprávnění je veden u vedoucí správy.
- V budově je ke zvýšení bezpečnosti osob, aktiv a majetku umístěn rámový průchozí detektor kovu, justiční stráž kontrolující vstup je rovněž vybavena ručním detektorem kovu.

Kontroly vstupu osob

Požadavek: *Aby bylo zajištěno, že je přístup do zabezpečených oblastí povolen pouze oprávněným osobám, měly by být tyto oblasti chráněny vhodným systémem kontrol vstupu.*

- Režim a kontrola pohybu osob v objektu OSZ **není stanovena** Návštěvním řádem a je založen na zvykovém pravidlu, kdy je jakákoliv návštěva OSZ doprovázena navštíveným zaměstnancem OSZ. Vstup do objektu OSZ je monitorován kamerovým systémem a okamžitě vyhodnocován příslušníkem justiční stráže. Je nutné stanovit režim a kontrolu vstupu osob ve formě písemného dokumentu, závazného pro všechny zaměstnance OSZ a službu konající příslušníky justiční stráže.

Zabezpečení kanceláří, místností a zařízení

Požadavek: *Mělo by být navrženo a aplikováno fyzické zabezpečení kanceláří, místností a zařízení.*

- Vstupy do kanceláří jsou zabezpečeny uzamykáním.

- Klíčový režim je realizován systémem generálního klíče. Klíč od vstupních dveří do prostor OSZ a své kanceláře mají všichni zaměstnanci trvale u sebe. Přehled evidence vydaných klíčů a vydaných přístupových oprávnění má vedoucí správy.
- Duplikáty klíčů jsou uloženy v uzamčené skříncev zabezpečené oblasti, včetně klíče generálního.
- Generální klíč má okresní státní zástupkyně, náměstkyně a pracovnice úklidu.
- Klíč od stanoviště justiční stráže mají službu konající příslušníci justiční stráže. Jeho duplikát je taktéž uložen v zabezpečené oblasti.

Ochrana před hrozbami vnějšího prostředí

Požadavek: *Na ochranu proti škodám způsobeným požárem, povodní, zemětřesením, výbuchem, civilními nepokoji a jinými přírodními nebo lidmi zapříčiněnými katastrofami by měly být navrženy a aplikovány prvky fyzické ochrany.*

- Je řešeno v rámci povinné dokumentace požární ochrany a Plánem krizové připravenosti OSZ. Pro řešení krizových situací lze využít i Plán zabezpečení objektů a zabezpečené oblasti v krizových situacích, zpracovaný v rámci projektu pokrývající ochranu utajovaných informací ze zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti.

➢ Bezpečnost zařízení

Cíl: *Předcházet ztrátě, poškození nebo kompromitaci aktiva přerušení činnosti organizace.*

Umístění zařízení a jeho ochrana

Požadavek: *Zařízení by měla být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.*

- Zařízení (kopírovací stroje a centrální tiskárny) jsou umístěna v kancelářích a v samostatné místnosti.

Bezpečnost zařízení mimo prostory organizace

Požadavek: *Zařízení používané mimo prostory organizace by mělo být zabezpečeno s přihlédnutím k různým rizikům vyplývajících z jejich použití mimo organizaci.*

- V rámci okresního státního zastupitelství je Provozním řádem počítačových sítí zakázáno připojování notebooku do sítě LAN.

Bezpečná likvidace nebo opakované použití zařízení

Požadavek: *Všechna zařízení obsahující paměťová média by měla být kontrolována tak, aby bylo možné zajistit, že před jejich likvidací nebo opakovaným použitím budou citlivá data a licencované programové vybavení odstraněna nebo přepsána.*

- V oblasti listinného zpracování informací je řešeno ve Skartačním řádu, kde je požadavek na znemožnění rekonstrukce informací a identifikace obsahu.
- V oblasti počítačového zpracování informací je řešeno V Ukládacím řádu agend vedených na počítačích.

U zařízení obsahujících osobní údaje by mělo být preferováno fyzické zničení nebo bezpečné smazání/přepsání dat za použití postupů znemožňujících jejich obnovu a to ještě před použitím běžné funkce mazání nebo formátování (například vhodným programovým prostředkem).

3.2.6 Řízení komunikace a provozu

➢ **Provozní postupy a odpovědnosti**

Cíl: *Zajistit správný a bezpečný provoz prostředků pro zpracování informací.*

Dokumentace provozních postupů

Požadavek: *Provozní postupy by měly být zdokumentovány a udržovány a měly by být dostupné všem uživatelům dle potřeby.*

- Provozní postupy v oblasti IT jsou formálně popsány v dokumentu Organizační opatření krajského státního zástupce, jímž se vydává Ukládací řád agend vedených na počítačích.

Řízení změn

Požadavek: *Změny ve vybavení a prostředcích pro zpracování informací by měly být řízeny.*

- Požadavky na změny v IT jsou plánovány a zdokumentovány ze strany nadřízeného krajského státního zastupitelství. Následně jsou pak vyhodnoceny.

- **Plánování a přejímání informačních systémů**

Cíl: *Minimalizovat riziko selhání informačních systémů.*

Řízení kapacit

Požadavek: *Pro zajištění požadovaného výkonu informačního systému, s ohledem na budoucí kapacitní požadavky, by mělo být monitorováno, nastaveno a projektováno využití zdrojů.*

- Výkon a zatížení informačního systému se sleduje ze strany nadřízené složky, za využití systémových nástrojů serverového operačního systému. Plánování potřebných kapacit informačního systému se periodicky a v souvislosti potřebou nákupu nových komponent.

- **Ochrana proti škodlivým programům a mobilním kódům**

Cíl: *Chránit integritu programů a dat.*

Opatření na ochranu proti škodlivým programům

Požadavek: *Na ochranu proti škodlivým programům a nepovoleným mobilním kódům by měla být implementována na jejich detekci, prevenci a nápravu a zvyšováno odpovídající bezpečnostní povědomí uživatelů.*

- Antivirová ochrana je řešena centrálně z úrovně Ministerstva spravedlnosti ČR

Opatření na ochranu proti mobilním kódům

Požadavek: *Použití povolených mobilních kódů by mělo být nastaveno v souladu s bezpečnostní politikou, mělo by být zabráněno spuštění nepovolených mobilních kódů.*

- Ochrana proti mobilním kódům, obdobně jako ochrana před škodlivými programy, je řešena centrálně.

- **Zálohování**

Cíl: *Udržovat integritu a dostupnost informací a prostředků pro jejich zpracování.*

Zálohování

Požadavek: *Záložní kopie důležitých informací a programového vybavení organizace by měly být pořizovány a testovány v pravidelných intervalech.*

- Na úrovni listinného zpracování informací se zálohování provádí na základě Kancelářského a Skartačního řádu. Na úrovni automatizovaného zpracování informací se provádí na základě Ukládacího řádu.
- Zálohování probíhá v prostorách serverovny na magnetické pásky, které jsou následně ukládané v trezoru. Zálohování provádí pověřený pracovník OSZ, odpovědným pracovníkem je informatik KSZ. Proces je popsán v Ukládacím řádu a pravidelně aktualizován formou organizačních opatření OSZ.

➢ **Bezpečnost při zacházení s médii**

Cíl: *Předcházet neoprávněnému prozrazení, modifikaci, ztrátě nebo poškození aktiv a přerušení činnosti organizace.*

Správa vyměnitelných počítačových

Požadavek: *Měly by být vytvořeny postupy pro správu vyměnitelných počítačových médií.*

- Problematika správy příloh je v oblasti listinných dokumentů řešena dostatečně v Kancelářském řádu.
- Problematika správy výměnných počítačových médií v oblasti IT je popsaná a zdokumentována v Ukládacím řádu. Evidence a sledování životnosti médií vede odpovědný informatik. Sady zálohovacích médií se mění s roční periodou, kdy se na tyto média uloží roční záloha a na zálohování se použije nová sada médií.

Postupy pro manipulaci s informacemi

Požadavek: *Pro zabránění neautorizovanému přístupu nebo zneužití informací by měla být stanovena pravidla pro manipulaci s nimi a pro jejich ukládání.*

- Tyto postupy jsou na úrovni listinného zpracování informací velmi kvalitně a detailně definovány Kancelářským řádem.
- V oblasti automatizovaného zpracování informací ale jsou definovány postupy v Ukládacím řádu a v Provozním řádu počítačových sítí.

- **Výměny informací**

Cíl: *Zajistit bezpečnost informací a programů při jejich výměně v rámci organizace a při jejich výměně s externími subjekty.*

Podnikové informační systémy

Požadavek: *Na ochranu informací v propojených podnikových informačních systémech by měla být vytvořena a do praxe zavedena politika a odpovídající směrnice.*

- Základní problematika a postupy jsou řešeny v Provozním řádu počítačových sítí.

- **Monitorování**

Cíl: *Detekovat neoprávněné zpracování informací.*

Zaznamenávání událostí

Požadavek: *Auditní záznamy, obsahující chybová hlášení a jiné bezpečnostně významné události, by měly být pořizovány a uchovány po stanovené období tak, aby byly se daly použít pro budoucí vyšetřování a pro účely monitorování řízení přístupu.*

- Události a činnosti se v rámci OSZ zaznamenávají, postup je uveden v Ukládacím řádu agend vedených na počítačích a částečně Provozním řádu počítačových sítí.

Monitorování používání systému

Požadavek: *Měla by být stanovena pravidla pro monitorování použití prostředků pro zpracování informací, výsledky těchto monitorování by měly být pravidelně přezkoumávány.*

- Pravidelné vyhodnocování a kontrola využití prostředků IT je prováděno periodicky, kdy je kladen důraz u systému ISYZ (program evidence trestních rejstříků).

Ochrana vytvořených záznamů

Požadavek: *Prostředky pro zaznamenávání informací a vytvořené záznamy by měly být vhodným způsobem chráněny proti neoprávněnému přístupu a zfalšování.*

- Požadavek je řešen v Provozním řádu počítačových sítí.

3.2.7 Řízení přístupu

- **Požadavky na řízení přístupu**

Cíl: *Řídit přístup k informacím.*

Politika řízení přístupu

Požadavek: *Měla by být vytvořena, dokumentována a v závislosti na aktuálních bezpečnostních požadavcích přezkoumávána politika řízení přístupu.*

- V oblasti listinného zpracování informací je politika řízení přístupu k informacím jasně dána Kancelářským řádem.
- V oblasti fyzického přístupu je přístup do objektu stanoven Návštěvním řádem.
- V oblasti IT je nastavena v Provozním řádu počítačových sítí.

- **Řízení přístupu uživatelů**

Cíl: *Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k informačním systémům.*

Registrace uživatele

Požadavek: *Měl by existovat postup pro formální registraci, včetně jejího zrušení, který zajistí autorizovaný přístup ke všem víceuživatelským informačním systémům a službám.*

- Procedury registrace uživatelů jsou ustaveny v Provozním řádu počítačových sítí, a to definováním přístupových rolí uživatelů podle konkrétních požadavků organizace.

Řízení privilegovaného přístupu

Požadavek: *Přidělování a používání privilegií by mělo být omezeno a řízeno.*

- Privilegovaný přístup je omezen výhradně na administrátory. Postupy jsou definovány v Provozním řádu počítačových sítí.

Správa uživatelských hesel

Požadavek: *Přidělování hesel by mělo být řízeno formálním procesem.*

- Uživatelská hesla jsou jednotlivým uživatelům přidělována podle stanovených rolí, požadavky na složitost hesla a jeho pravidelnou obměnu jsou definovány.

Přezkoumání přístupových práv uživatelů

Požadavek: *Vedení organizace by mělo v pravidelných intervalech provádět formální přezkoumání přístupových práv uživatelů.*

Přístupová práva jsou u organizace přezkoumávána v pravidelných intervalech (interval 6 měsíců), a dále okamžitě po každé změně v pracovním zařazení uživatele, jako například povýšení, přeložení na jinou pozici nebo ukončení pracovního poměru.

➢ Odpovědnosti uživatelů

Cíl: *Předcházet neoprávněnému uživatelskému přístupu, prozrazení nebo krádeži informací a prostředků pro zpracování informací.*

Používání hesel

Požadavek: *Při výběru a používání hesel by mělo být po uživatelích požadováno, aby dodržovali stanovené bezpečnostní postupy.*

- Používání hesla je povinné, struktura hesla a jeho pravidelná obměna (1x za 2 měsíce) je stanovena. Dále je stanoven požadavek na udržování hesla v tajnosti.

Neobsluhovaná uživatelská zařízení

Požadavek: *Uživatelé by měli zajistit přiměřenou ochranu neobsluhovaných zařízení.*

- Pro neobsluhovaná zařízení je stanoveno povinné používání „šetřiče obrazovky“.
- Uživatelé jsou instruováni o povinnosti odhlásit se, když odcházejí od počítače.

Zásada prázdného stolu a prázdné obrazovky monitoru

Požadavek: *Měla by být přijata zásada prázdného stolu ve vztahu k dokumentům a vyměnitelným médiím a zásada prázdné obrazovky monitoru u prostředků pro zpracování informací.*

- Pro tuto problematiku jsou stanovena pravidla („šetřič“ obrazovky, zamknutí obrazovky, odhlášení). Pravidlo čistého stolu **není** u organizace zavedeno.

- **Řízení přístupu k síti**

Cíl: *Předcházet neautorizovanému přístupu k síťovým službám.*

Politika užívání síťových služeb

Požadavek: *Uživatelé by měli mít přímý přístup pouze k těm síťovým službám, pro jejichž použití byli zvlášť oprávněni.*

- Přístup k síťovým službám je v organizaci řízen,

Ochrana portů pro vzdálenou diagnostiku a konfiguraci

Požadavek: *Fyzický i logický přístup k diagnostickým a konfiguračním portům by měl být bezpečně řízen.*

- Fyzický přístup k portům je zabezpečen omezením přístupu osob do prostor IT. Logický přístup k diagnostickým a konfiguračním portům je zabezpečen z úrovně MSp. Tyto pravidla a postupy jsou dokumentačně podchyceny.

- **Řízení přístupu k operačnímu systému**

Cíl: *Předcházet neautorizovanému přístupu k operačním systémům.*

Bezpečné postupy přihlášení

Požadavek: *Přístup k operačnímu systému by měl být řízen postupy.*

- Postupy bezpečného přihlášení jsou v organizaci implementovány na úrovni přihlášení heslem. Síla hesla i jeho obměňování jsou jasně stanoveny.

Identifikace a autentizace uživatelů

Požadavek: *Všichni uživatelé by měli mít pro výhradní osobní použití jedinečný identifikátor (uživatelské ID), měl by být také zvolen vhodný způsob autentizace k ověření jejich identity.*

- Požadavek je v organizaci implementován. Neexistují univerzální konta.

Systém správy hesel

Požadavek: *Systém správy hesel by měl být interaktivní a měl by zajišťovat použití kvalitních hesel.*

- Požadavek je v organizaci implementován. Je stanoveno používání individuálních hesel a uživatelských ID pro udržení odpovědnosti uživatelů. Uživatelům je umožněno volit a měnit si své vlastní heslo podle nastavených pravidel.

Použití systémových nástrojů

Požadavek: *Použití systémových nástrojů, které jsou schopné překonat systémové nebo aplikační kontroly by mělo být omezeno a přísně kontrolováno.*

- Požadavek je sice v organizaci implementován, ale principy nejsou stanoveny, ani popsány. Omezení požití systémových nástrojů vychází spíše z tradice, takže není striktně vymahatelné. Není definováno, ke kterým systémovým nástrojům má být omezen přístup, ani kdo je oprávněn je používat. Omezení je realizováno na základě úsudku administrátora.

➢ Řízení přístupu k aplikacím a informacím

Cíl: *Předcházet neoprávněnému přístupu k informacím uloženým v počítačových systémech.*

Omezení přístupu k informacím

Požadavek: *Uživatelé aplikačních systémů, včetně pracovníků podpory, by měli mít přístup k informacím a funkcím aplikačních systémů omezen v souladu s definovanou politikou řízení přístupu.*

- V oblasti listinného zpracování informací je řízení přístupu k informacím stanoveno Kancelářským řádem.
- V oblasti informačních systémů je zavedeno řízení přístupu uživatelů na úrovni soukromých a sdílených adresářů. Pravidla definována jsou v organizačních opatřeních.
- U systémů se vzdáleným přístupem (např. Centrální evidence obyvatel) jsou mechanismy omezení přístupu k informacím implementovány.

➢ Mobilní výpočetní zařízení a práce na dálku

Cíl: *Zajistit bezpečnost informací při použití mobilní výpočetní techniky a při využití zařízení pro práci na dálku.*

Mobilní výpočetní zařízení a sdělovací technika

Požadavek: *Měla by být ustavena formální pravidla a přijata na ochranu proti rizikům použití mobilních výpočetních a komunikačních zařízení.*

- Pravidla pro používání mobilní techniky u organizace jsou stanoveny v dokumentu Provozní řád počítačových sítí, kde je zákaz připojování přenosných počítačů do sítě LAN.

3.2.8 Zvládání bezpečnostních incidentů

➢ **Hlášení bezpečnostních událostí a slabin**

Cíl: *Zajistit nahlášení bezpečnostních událostí a slabin informačního systému způsobem, který umožní včasné zahájení kroků vedoucích k nápravě.*

Požadavek: *Bezpečnostní události by měly být hlášeny příslušnými řídícími cestami tak rychle, jak je to jen možné. Všichni zaměstnanci, smluvní strany a další nespecifikovaní uživatelé informačního systému a služeb by měli být povinni zaznamenat a hlásit jakékoliv bezpečnostní slabiny nebo podezření na bezpečnostní slabiny v systémech nebo službách.*

- Opatření je realizováno v Provozním řádu počítačových sítí. Pro hlášení bezpečnostní události je vytvořen formalizovaný postup, včetně postupu reakce na incidenty, definující činnosti, které mají být po přijetí hlášení provedeny. Uživatelé jsou informováni o tom, že za žádných okolností nesmí prověřovat bezpečnostní události, ale musí je pouze okamžitě hlásit.

➢ **Zvládání bezpečnostních incidentů a kroky k nápravě**

Cíl: *Zajistit odpovídající a účinný přístup ke zvládání bezpečnostních incidentů.*

Odpovědnosti a postupy

Požadavek: *Pro zajištění rychlé, účinné a systematické reakce na bezpečnostní incidenty by měly být zavedeny odpovědnosti a postupy pro zvládání bezpečnostních incidentů.*

- Opatření je formálně realizováno, a to v oblasti listinného zpracování v dokumentu Kancelářský řád a v oblasti IT v dokumentu Provozní řád počítačových sítí.

Ponaučení z bezpečnostních incidentů

***Požadavek**: Měly by existovat mechanizmy, které by umožňovaly kvantifikovat a monitorovat typy, rozsah a náklady bezpečnostních incidentů.*

- Opatření je částečně řešeno v Provozním řádu počítačových sítí. Opatření je důležité, neboť informace získané při vyhodnocení bezpečnostních incidentů mohou být využity pro identifikaci opakujících se incidentů nebo incidentů s velkými následky. Závěry z vyhodnocení bezpečnostních incidentů mohou také signalizovat potřebu využití dodatečných nebo důkladnějších opatření, která by omezila frekvenci, škody a náklady jejich budoucích výskytů.

Shromaždování důkazů

***Požadavek:** V případech, kdy vyústění bezpečnostního incidentu směřuje k právnímu řízení (dle práva občanského nebo trestního) vůči osobě nebo organizaci, by měly být sbírány, uchovávány a soudu předkládány důkazy v souladu s pravidly příslušné jurisdikce, kde se bude případ projednávat.*

- Lze částečně využít všechna ustanovení v Provozním řádu počítačových sítí.

3.2.9 Soulad s požadavky

➢ **Soulad s právními normami**

***Cíl:** Vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.*

Ochrana záznamů organizace

***Požadavek:** Důležité záznamy organizace by měly být chráněny proti ztrátě, zničení a padělání, a to v souladu se zákonnými, podzákonnými a smluvními požadavky a požadavky organizace.*

- Ochrana záznamů v oblasti listinného zpracování informací je řešena Kancelářským a Skartačním řádem.
- V oblasti automatizovaného zpracování informací je řešení v Provozním řádu počítačových sítí.

Prevence zneužití prostředků pro zpracování informací

Požadavek: *Mělo by být zakázáno používat prostředky pro zpracování informací jiným než autorizovaným způsobem.*

- V oblasti administrativní bezpečnosti jsou prováděny kontroly a prověrky spisů.
- V oblasti IT vyplývá prevence z komplexu ostatních opatření. **Neprovádí se** pravidelné školení zaměstnanců.

➢ **Soulad s bezpečnostními politikami, normami a technická shoda**

Cíl: *Zajistit shodu systémů s bezpečnostními politikami organizace a normami.*

Shoda s bezpečnostními politikami a normami

Požadavek: *Vedoucí zaměstnanci by měli zajistit, aby všechny bezpečnostní postupy v rozsahu jejich odpovědnosti byly prováděny správně, v souladu s bezpečnostními politikami a normami.*

- Shoda s normami se kontroluje, je uložena povinnost dodržování interních nařizovacích aktů.

Kontrola technické shody

Požadavek: *Informační systémy by měly být pravidelně kontrolovány, zda jsou v souladu s bezpečnostními politikami a standardy.*

- Technická shoda je prováděna nadřízenými složkami v rámci centrálního zásobování technikou.

- **Hlediska auditu informačních systémů**

Cíl: *Maximalizovat účinnost auditu a minimalizovat zásahy do informačních systémů.*

Opatření k auditu informačních systémů

Požadavek: *Požadavky auditu a činnosti zahrnující kontrolu provozních systémů by měly být pečlivě naplánovány a schváleny, aby se minimalizovalo riziko narušení činností organizace.*

- Je realizován pravidelně se opakující audit a je zabezpečeno provádění auditu bezpečnosti IT odborně znalými specialisty.

Ochrana nástrojů pro audit informačních systémů

Požadavek: *Přístup k nástrojům určeným pro audit informačních systémů by měl být chráněn, aby se předešlo jejich možnému zneužití nebo ohrožení.*

- Přístup a ochrana je popsána v Organizačním řádu, Provozním řádu počítačových sítí a Ukládacím řádu počítačových agend.

3.3 Vyhodnocení rizik

V souladu s § 13 odst. 1 zákona č. 101/2000 Sb. je správce i zpracovatel povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zneužití či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

K zabezpečení tohoto je nutné provést posouzení rizik v minimálním rozsahu určeném v § 13 odst. 3 zákona.

Jedná se konkrétně o posouzení rizika týkající se:

- plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům (principy autorizace),
- zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování (princip důvěrnosti a dostupnosti),
- zabránění neoprávněnému čtení, vytváření, kopírování, přenosu úpravě či vymazání záznamů obsahujících osobní údaje (princip důvěrnosti a integrity),
- opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

Při stanovení a vyhodnocení rizik jsem vycházela z posouzení současného stavu jednotlivých oblastí bezpečnosti ve vztahu ke zpracovaným a zavedeným opatřením a z kvalifikovaného odhadu vedoucích zaměstnanců, kteří stanovili pravděpodobnost vzniku možného ohrožení informace.

Rizika při plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k údajům

Hrozba rizika při plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k údajům představuje úmyslné nebo neúmyslné porušení povinností. Jedná se především o tyto formy rizik:

- neznalost správných postupů,
- nedostatečně definované procedury nakládání s osobními údaji,
- nedbalost,
- úmyslný čin.

Velikost rizika závisí na zavedených opatřeních organizace a uvědomění jednotlivých osob:

- stanovení povinnosti dodržovat ustanovení Zákona,
- stanovení postupů k nakládání s osobními údaji,
- právní a bezpečnostní povědomí osob,
- loajalita.

Výše popisované naplnění formy rizika jsou částečně minimalizována určitou praxí a loajalitou osob. Naplnění rizika však nelze vyloučit, a to zejména za finanční odměnu, případně jiné materiální plnění, potom je naplnění rizika reálné. Rovněž nelze vyloučit vyzrazení informace osobami, kterým je vyhrožováno použitím násilí nebo pohrůžkou použití násilí vůči jejich rodinným příslušníkům. Může jít o porušení režimových opatření, např. nezabezpečení informace všemi technickými prostředky určenými k jejich ochraně, nedbalostí při prováděné skartaci. Toto riziko se dá zčásti eliminovat pečlivým výběrem zaměstnanců, jejich periodickým proškolováním a důslednou kontrolou dodržování režimu stanoveného pro manipulaci s informacemi, resp. osobními údaji. Nikdy však nelze vyloučit selhání jednotlivce, kterému lze částečně předcházet pravidelným školením.

Míra naplnění rizika při plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k údajům je stanovena jako **střední**.

Rizika v přístupu neoprávněných osob k osobním údajům a k prostředkům pro jejich zpracování

Hrozba rizika v přístupu neoprávněných osob k osobním údajům a k prostředkům pro jejich zpracování může nastat následkem:

- oprávněného vstupu povolané osoby nemající právo seznamovat se s osobními údaji (např. pracovník úklidu),
- oprávněného vstupu nepovolané osoby (např. návštěva),
- neoprávněného vstupu neoprávněnou osobou (např. vloupání).

Velikost rizika je ovlivněno nastavením opatření týkajícím se fyzické bezpečnosti, kterými jsou:

- režim návštěv,
- režim ukládání a zacházení s osobními údaji,
- fyzické zabezpečení objektu a režim ostrahy,

K riziku přístupu neoprávněných osob k osobním údajům a k prostředkům pro jejich zpracování může dojít např. zcizením volně ponechaných informací bez dozoru nebo jejich ztrátou. Riziko překonání technických prostředků, vloupání a odcizení informací nelze u OSZ nikdy zcela vyloučit. Příčinou vloupání nemusí být jen snaha získat informace, ale i možnost krádeže movitých věcí. Budova je však vybavena elektrickým zabezpečovacím systémem, určeným k signalizaci pokusu o neoprávněný vstup a kamerovým systémem sloužícím k identifikaci případných pachatelů. Riziko loupežného přepadení osoby je na malé úrovni. Riziko se dá omezit přesně danými pravidly o pohybu nepovolaných osob (návštěv) v budově, která však nejsou u OSZ nastavena. Riziko neoprávněného seznámení s osobními údaji uklízečkou lze eliminovat opatřením, které stanoví přesný režim provádění úklidu. **Míra naplnění rizika** v přístupu neoprávněných osob k osobním údajům a k prostředkům pro jejich zpracování je stanovena jako **velká**.

Rizika při zabránění neoprávněnému vytváření, kopírování, přenosu, úpravě, či vymazání záznamů obsahujících osobní údaje

Hrozba rizika při zabránění neoprávněnému vytváření, kopírování, přenosu, úpravě, či vymazání záznamů obsahujících osobní údaje může nastat následkem:

- nedostatečného zabezpečení prostředků pro zpracování a kopírování informací,
- nedostatečnými pravidly pro nakládání s OÚ a prostředky pro zpracování OÚ,
- porušením pracovních povinností.

Na velikost rizika mají vliv zavedená opatření týkající se :

- zabezpečení prostředků pro zpracování a kopírování informací,
- bezpečnostního vědomí zaměstnanců,
- stanovených pravidel pro nakládání s informacemi a prostředky pro zpracování informací.

Riziko při zabránění neoprávněnému vytváření, kopírování, přenosu, úpravě, či vymazání záznamů obsahujících osobní údaje, nelze nikdy zcela vyloučit. Jeho velikost závisí právě na stanovení jasných pravidel, jejich dodržováním jednotlivými osobami, stejně jako důslednou kontrolou plnění povinností. Kopírovací zařízení a centrální tiskárny jsou v kancelářích jednotlivých pracovníků nebo ve speciálních místnostech, je zaveden systém pravidelných kontrol. Organizační opatření jsou z tohoto pohledu dostatečná nastavena, vyjma doby úklidu, kdy může dojít k neoprávněnému seznámení v případě volně ponechaného dokumentu s osobními údajů. **Míra naplnění rizika** při zabránění neoprávněnému vytváření, kopírování, přenosu, úpravě, či vymazání záznamů obsahujících osobní údaje je **malá**.

Rizika týkající se procesu manipulace nebo předávání osobních údajů jednotlivými osobami, včetně identifikace těchto osob

Hrozba rizika týkající se procesu manipulace nebo předávání osobních údajů jednotlivými osobami, včetně identifikace těchto osob může nastat důsledkem:

- nezaznamenání manipulace s informací,
- nedostatečným stanovením odpovědnosti,
- ztrátou nebo zničením auditních záznamů z IS,
- nedostatečnými pravidly pro nakládání s osobními údaji.

Velikost rizika lze částečně eliminovat:

- stanovením pravidel pro nakládání s informacemi,
- nastavením auditu v IS,
- archivací a vyhodnocováním auditních záznamů,
- zabezpečením prostředků pro zpracování a kopírování informací.

Rizika týkající se procesu manipulace nebo předávání osobních údajů jednotlivými osobami, včetně identifikace těchto osob spočívá v nastavení jasně stanovených pravidel. Nelze vyloučit riziko při zpracování osobních údajů spočívající v opomenutí při přidělování nebo rušení přístupových práv jednotlivým osobám. Riziko lze eliminovat systematickým prováděním kontrol a soustavným proškolováním pracovníků. **Míra rizika** týkající se procesu manipulace nebo předávání osobních údajů jednotlivými osobami, včetně identifikace těchto osob je stanovena jako **střední**.

Stanovení míry rizika

Tabulka č. 1

Hrozba	Míra rizika
při plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k údajům	střední
v přístupu neoprávněných osob k osobním údajům a k prostředkům pro jejich zpracování	velká
při zabránění neoprávněnému vytváření, kopírování, přenosu, úpravě, či vymazání záznamů obsahujících osobní údaje	malá
týkající se procesu manipulace nebo předávání osobních údajů jednotlivými osobami, včetně identifikace těchto osob	střední

Z vyhodnocení rizik vyplývá, že největší rizika spočívají v procesu manipulace nebo předávání osobních údajů jednotlivými osobami, včetně identifikace těchto osob. Druhým největším rizikem je zabezpečení povinnosti zabránění neoprávněnému vytváření, kopírování, přenosu, úpravě, či vymazání záznamů obsahujících osobní údaje.

K eliminaci rizik jsou v následující kapitole ve smyslu § 13 odst. 1 Zákona navrhována taková organizační opatření, která mají zabránit k neoprávněnému nebo nahodilému přístupu k osobním údajům a k prostředkům pro jejich zpracování a následkem toho k neoprávněné manipulaci s nimi, jakož i k jinému zneužití osobních údajů.

3.4 Výsledky analýzy, souhrn nejzávažnějších nedostatků

Optimální bezpečnostní řešení vždy je nutné navrhovat individuálně podle konkrétních podmínek, kdy je jeho součástí také stanovení bezpečnostních pravidel a zavedení patřičných technických i organizačních opatření.

Vzhledem k charakteru činnosti okresního státního zastupitelství byly hodnoceny informace zpracovávané v listinné podobě (někdy se hovoří o neautomatizovaném zpracování informací) a informace zpracovávané v informačních systémech (automatizované zpracování informací). Z posouzení stávajícího stavu ochrany osobních údajů vyplynuly závěry, které ukazují na potřebu upřesnění zavedených opatření, aby byla naplněna ustanovení Zákona.

Výsledky provedené analýzy vypovídají o faktu, že se některé bezpečnostní opatření provádí neformálně (zvykově) a není nijak popsáno. S tím souvisí také vymahatelnost takového opatření. Jestliže není opatření popsáno a není v žádném dokumentu ustanovena povinnost toto opatření realizovat, je nevymahatelné a jeho realizace závisí pouze na dobré vůli a pečlivosti zaměstnanců.

V analýze problému současné situace jsou rozepsány a hodnoceny jednotlivé oblasti bezpečnosti, uvedené cíle slouží pouze k jejich zatřídění do logických celků. vzhledem k velkému počtu oblastí jsou nedostatky uvedeny přímo v posouzení stávajícího stavu, neboť v konkrétní chvíli byly takto zavedeny v praxi. Z analýzy ochrany osobních údajů však nakonec vyplynulo několik nedostatků, které je třeba odstranit, aby bylo eliminováno riziko případného zneužití osobních údajů a bylo splněno stanovení § 13 odst. 1 Zákona.

V rámci posuzování současného stavu ochrany osobních údajů u okresního státního zastupitelství byly **vyhodnoceny tyto nedostatky**:

1) Úklid kanceláří je prováděn vlastním pracovníkem, ale bez přítomnosti daného vlastníka aktiv, přičemž není dodržována zásada „čistého stolu“. *(oblast organizace bezpečnosti)*

Úklid kanceláří je prováděn vlastními zaměstnanci, zásadně po pracovní době, vždy bez přítomnosti daného vlastníka aktiv (kanceláře). Zaměstnanec provádějící úklid má podepsaný závazek o mlčenlivosti, přesto vzniká značné riziko neoprávněného přístupu k osobním údajům a jiným citlivým informacím.

2) Neexistuje soustavný systém školení pracovníků v zajišťování bezpečnosti informací. *(oblast bezpečnosti lidských zdrojů)*

U okresního státního zastupitelství je zaveden systém školení v oblasti bezpečnosti, ochrany zdraví a práce, v oblasti požární bezpečnosti a ochrany utajovaných informací. Dále je zaveden systém školení týkající se odborných kompetencí v souvislostí s vykonávanou funkcí. Ostatní školení probíhají pouze na základě zájmu jednotlivých pracovníků a jejich účast závisí na vydání souhlasu nadřízeného pracovníka.

3) Není stanoven režim návštěv a kontroly vstupu ve formě písemného dokumentu, závazného pro všechny zaměstnance OSZ a službu konající příslušníky justiční stráže. *(oblast fyzické bezpečnosti a bezpečnosti prostředí)*

Vstup do budovy je monitorován kamerovým systémem a okamžitě vyhodnocován službu konajícím příslušníkem justiční stráže. Návštěva se prokazuje platným průkazem totožnosti, její příchod a odchod je zaevidován do knihy návštěv. Pro průběh návštěvy platí zvykové pravidlo, kdy konkrétní zaměstnanec vyzvedne návštěvu na stanovišti justiční stráže a při odchodu ji doprovodí zpět. V návštěvním řádu není písemně stanoven režim návštěv, proto nelze uplatnit princip vymahatelnosti při jeho porušení. Současně je zde riziko seznámení neoprávněné osoby s osobními údaji.

4) Není explicitně ustanovena osoba, která by řídila a koordinovala bezpečnost informací. *(oblast organizace bezpečnosti)*

Přestože ustanovení osoby, která by komplexně zajišťovala celou oblast bezpečnosti není Zákonem uloženo, je vhodné takovou osobu určit. Její ustanovení by mohlo být prvním krokem k realizaci bezpečnostní politiky, která není u okresního státního zastupitelství formulována, ale je obsažena v samostatných interních nařizovacích aktech. Tím je způsobeno, že jakákoli změna v přístupu k řešení bezpečnosti musí být promítána do jednotlivých dokumentů, což má za následek větší pravděpodobnost opomenutí promítnutí požadované změny ve všech dokumentech, kterých se problematika bezpečnosti týká.

Osobou odpovědnou za oblast bezpečnosti se stanovenými kompetencemi v rámci celého okresního státního zastupitelství by mohl být bezpečnostní ředitel, který již nyní odpovídá za většinu oblastí týkajících se bezpečnosti.

4 Vlastní návrhy řešení, přínos návrhů řešení

Manažerský pohled

Smyslem manažerského shrnutí je poskytnout zobecněný pohled na bezpečností problematiku.

Principy ochrany osobních údajů vycházejí z obecných principů používaných pro bezpečnost informací, které jsou vztaženy na jednu zvláštní kategorii informací, a to na osobní údaje. Prostřednictvím tohoto zobecnění se dostaneme na úroveň, která nám umožní pochopit, že vytvoření jednotného systému řízení bezpečnosti informací u okresního státního zastupitelství vytvoří ty nejlepší předpoklady pro ochranu osobních údajů.

Odstranění zjištěných nedostatků musí mít nejvyšší prioritu, neboť v souladu s § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. (PO nebo FO která nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů) hrozí sankce ve výši dle § 45 odst. 3 až do výše 5 miliónů Kč, v případech zpracování citlivých osobních údajů sankce dle § 45 odst. 4 až do výše 10 miliónů Kč.

Návrhy řešení

Optimální bezpečnostní řešení je nutno navrhovat vždy individuálně podle konkrétních podmínek. Součástí řešení je stanovení bezpečnostních pravidel a zavedení patřičných technických i organizačních opatření, čehož bylo v této práci dosaženo.

Doporučení návrhů řešení směřuje ke zpracování chybějících, případně doplnění již platných, interních nařizovacích aktů. Při řešení návrhů jsem vycházela z nedostatků uvedených v analýze současného situace okresního státního zastupitelství ve vztahu ke zjištěné míře jednotlivých rizik.

1) Úklid kanceláří – návrh řešení:

První možností je vydání opatření s provedením změny režimu úklidu, který se bude provádět vždy v pracovní době a vždy za přítomnosti vlastníka aktiv – uživatele kanceláře s tím, že současně bude písemně formulováno pravidlo „čistého stolu“, které je významným prvkem posílení bezpečnosti, kdy je minimalizováno riziko seznámení neoprávněné osoby (uklízečce) s osobními údaji.

Druhým způsobem je vydání opatření, které zachová stávající způsob úklidu, tj. po pracovní době bez přítomnosti vlastníka aktiv, ale bude v něm písemně zakotvena povinnost uzamykat všechny dokumenty s osobními údaji do skříní (klíče nesmí být ponechány v zámku), včetně dodržování pravidla tzv. „čistého stolu“.

Samozřejmostí by mělo být následné provádění namátkových kontrol zaměřených na dodržování vydaného opatření.

Cenová kalkulace

Náklady inovačního procesu spočívají pouze v administrativních úkonech ze strany vedení okresního státního zastupitelství. **Náklady na realizaci opatření: 0,00 Kč**

1) Systém školení – návrh řešení:

Možným řešením je zavedení uceleného systému školení pracovníků, který lze řešit vlastním pracovníkem nebo dodavatelsky odbornými firmami, a to buď přímým (fyzickou účastí) školením nebo formou e-learningu. Se specializovanou firmou je možné uzavřít smlouvu, která by obsahovala ustanovení nejen s podrobnostmi o konkrétním školení, jeho rozsahu, ale např. i povinnost informovat stanovenou osobu o změnách v právních předpisech a novinkách. Se systémem školení, dle mého názoru úzce souvisí neexistence bezpečnostní politiky a určení konkrétní osoby, která by se celou problematikou zabývala komplexně.

Odpovědnost za průběh a realizaci školení by měla nést vedením organizace pověřená konkrétní osoba, např. vedoucí personálního oddělení (v podmínkách OSZ je to vedoucí správy), která by současně zajišťovala absolvování školení u nově přijatých zaměstnanců.

Školení by mělo být prováděno **pravidelně 1x za rok**, s tím že v případě legislativní změny v oblasti osobních údajů, jsou všichni zaměstnanci s touto změnou seznámeni, což stvrdí svým podpisem (např. do protokolu o seznámení se s konkrétní změnou). Zaměstnanci musí být rovněž vždy prokazatelně (proti podpisu) seznámeni s každým novým organizačním opatřením OSZ a nadřízené složky KSZ.

Možný obsah a struktura školení:

- předpisy v oblasti ochrany osobních údajů,
- vymezení osobních údajů,
- zpracování osobních údajů,
- povinnosti při zpracování osobních údajů,
- práva subjektů údajů,
- odpovědnost a sankce,
- přehled a stručný obsah platných organizačních opatření OSZ.

Cenová kalkulace

Finanční prostředky směřované do vzdělání vlastních zaměstnanců jsou výhodnou investicí neboť každý pracovník vybavený potřebnými znalostmi a dovednosti je pro každého zaměstnavatele přínosem. V současné době se vyskytuje na trhu mnoho firem, které nabízejí shodné produkty v oblasti bezpečnosti, proto je i cena školení cenou, o které lze smlouvat. Dnes v tomto směru hraje roli i ekonomická krize a s tím související krácení rozpočtů státním institucím, takže i nabídka cen služeb jde zákonitě směrem dolů.

a) Hromadného školení v budově OSZ:

Školení lze různě kombinovat a dle potřeby organizace ho zaměřit na oblast ochrany osobních údajů, a to např. s důrazem na personální, administrativní či fyzickou bezpečnost, nebo bezpečnost informačního systému. Na školení je vhodné uvádět různé příklady z praxe a školené osoby upozorňovat na nedostatky, které se nejčastěji vyskytují při práci s osobními údaji. Účastníci školení mohou obdržet poznámkový sešit. Na základě prezenční listiny pak firma vystaví potvrzení každému účastníkovi, které organizace založí do osobního spisu zaměstnance. Školení je možné realizovat formou přednášky, která může mít současně podobu prezentace v PowerPointu.

Náklady na realizaci:

- školení v délce trvání 3 hodiny a cena na 1 osobu: 350,00 Kč bez DPH
- 11 osob OSZ: 3.850,00 Kč bez DPH
- **celkem: 4.815,50 Kč s DPH**

b) Školení organizované agenturou v jiných prostorách:

Forma školení může být shodná jako v předchozím bodě c) s tím, že na akcích pořádaných agenturou jsou přednášející často z řad uznávaných odborníků, a to přímo

z Úřadu pro ochranu osobních údajů nebo z řad osob, které se přímo podílely na tvorbě legislativy pro příslušnou oblast. Tato skutečnost se pak odráží i na výsledné ceně školení. Výhodou je, že organizace nemusí zajišťovat prostory, termíny konání, osvědčení o absolvování školení apod. V tomto případě stačí pouze zaslat přihlášku a uhradit účastnický poplatek.

Náklady na realizaci:

- délka školení 3 hodiny a na cena za 1 osobu: 990,00 Kč bez DPH
- 11 osob OSZ: 10.890 Kč bez DPH
- **celkem: 12.959,00 Kč s DPH**

c) Školení formou e-learningu:

Školení formou e-learningového kurzu zaměřené na problematiku ochrany osobních údajů je vhodné realizovat s úpravami dle potřeby organizace a zapracovat do něho požadavky jejího vedení týkající se konkrétní praxe. Cílem je seznámit zaměstnance s problematikou ochrany osobních údajů, zejména vysvětlit pojem osobní údaj, povinnosti při zpracování osobních údajů a práva subjektů údajů. Zpracování kurzu může mít podobu kvizových otázek v atraktivním grafickém podání. Délka studia kurzu je cca 30 minut.

Náklady na realizaci:

- 1 osoba: 250,00 Kč
- 11 osob OSZ: 2.750,00 Kč bez DPH
- **celkem: 3.273,00Kč s DPH**

2) Režim návštěv – návrh řešení:

Předpoklad efektivní ochrany osobních údajů v průběhu pohybu cizích subjektů (návštěv) v budově okresního státního zastupitelství spočívá v doplnění režimu průběhu návštěvy do návštěvního řádu.

Příklad možného znění:

- Návštěva předloží průkaz totožnosti justiční stáži.
- Justiční stráž návštěvu zaeviduje do knihy návštěv, kde je vyznačeno datum návštěvy, jméno návštěvy, číslo průkazu totožnosti, jméno navštíveného zaměstnance.

- Justiční stráž provede kontrolu ručním detektorem kovu (návštěva odloží kovové předměty, případné ostré předměty – nože zanechá proti potvrzení v úschově na stanovišti justiční stráže, nosit střelné zbraně je do prostor budovy zakázáno).
- Justiční stráž přivolá příslušného zaměstnance, který si návštěvu vyzvedne.
- Navštívený zaměstnanec odpovídá za návštěvu po celou dobu jejího průběhu.
- Navštívený zaměstnanec je po skončení jednání povinen návštěvu doprovodit na stanoviště justiční stráže.
- Justiční stráž vyznačí odchod návštěvy z budovy (vrátí případně předměty z úschovy).
- Zaměstnanci uvedení v poznámce se neevidují, ale prokazují služebním průkazem, a po telefonickém ohlášení jejich příchodu příslušnému zaměstnanci okresního státního zastupitelství je jim umožněn vstup do budovy.

(Poznámka: Návštěvou se rozumí přítomnost osoby, která není zaměstnancem okresního státního zastupitelství, Krajského státního zastupitelství v Brně nebo státního zastupitelství v obvodu jeho působnosti a která se dostavila v záležitosti související s výkonem působnosti státního zastupitelství nebo jeho správou anebo ze soukromých důvodů).

Cenová kalkulace

Náklady spočívají pouze v administrativních úkonech ze strany vedení okresního státního zastupitelství. **Náklady na realizaci opatření: 0,00 Kč**

3) Bezpečnostní politika – návrh řešení:

V rámci koordinace celé oblasti bezpečnosti považuji za nejlepší řešení ustanovit osobu, která by měla stanovené kompetence v rámci celého okresního státního zastupitelství. Touto osobou by mohl být bezpečnostní ředitel, který již v současné době odpovídá za dílčí úseky bezpečnosti. To, co okresnímu státnímu zastupitelství chybí, je vrcholový bezpečnostní dokument, který by jednotně nastavil systém řízení bezpečnosti, a tak komplexně zastřešil celou problematiku a stanovil obecná pravidla, jak bezpečnost řešit. Takovým dokumentem by měla být Bezpečnostní politika okresního státního zastupitelství. Dokument by vytvořil jednotný systém, stanovil by bezpečnostní management, garanty za jednotlivé oblasti bezpečnosti a nastavil by hlavní bezpečnostní procesy.

Hlavním problémem OSZ je roztříštěnost řešení problematiky bezpečnosti. Bezpečnost byla řešena podle toho, jak vznikaly potřeby řešit tu či onu problematiku

bezpečnosti a v neposlední řadě podle toho, jak vycházely jednotlivé legislativní předpisy. Vznikaly tak „ostrůvky“, kde je nějakým způsobem řešena určitá oblast bezpečnosti.

Takový přístup není ze systémového hlediska zrovna ideální. Pokud s každým právním předpisem, který se týká bezpečnosti, bude vznikat samostatná oblast řešení bezpečnostní problematiky a samostatný bezpečnostní management pro tuto oblast, vznikne s přibývající bezpečnostní legislativou změť bezpečnostních předpisů a nařízení, která bude nejen nepřehledná, ale jednotlivé předpisy v ní si mohou časem také protiřečit. K řešení bezpečnosti je zapotřebí komplexní přístup.

Podle mého názoru, systémově správný přístup je rozdělení problematiky bezpečnosti na jednotlivé oblasti, jako například na:

- řízení a koordinace bezpečnosti,
- bezpečnost informací a informačních systémů,
- personální bezpečnost,
- fyzickou bezpečnost,
- technickou a technologickou bezpečnost,

a tím vytvořit systém řízení bezpečnosti, který stanoví obecná pravidla, jak v jednotlivých oblastech řešit bezpečnost. Pokud v takových podmínkách přijde nový legislativní požadavek na bezpečnost, není potřeba vytvářet další oblast řešení bezpečnosti, ale požadavek se pouze integruje do stávajícího bezpečnostního systému.

Současně je vhodné zavést plán kontrolní činnosti směřované do oblasti povinností osob při zabezpečení potřebné ochrany osobních údajů (pro listinné tak i automatizované zpracování) jako součást bezpečnostní politiky.

Cenová kalkulace

Vytvoření bezpečnostní politiky je základním předpoklad pro komplexní přístup k bezpečnosti. Vyžaduje experty, kteří se celou problematikou bezpečnosti zabývají. Formulování bezpečnostní politiky zpracovat vlastními silami, resp. vlastními zaměstnanci nebo dodavatelsky, tzn. odbornou firmou.

Náklady na realizaci vlastními zaměstnanci: 0,00 Kč

Náklady na realizaci odbornou firmou: 110.000,00 Kč až 140.000,00 Kč bez DPH

130.900,00 Kč až 166.600,00 Kč s DPH

Náklady jsem zpracovala na základě telefonických konzultací se zástupci tří firem, které se zabývají problematikou ochrany osobních údajů.

Cenová kalkulace předpokládaných nákladů na realizaci navržených opatření (s DPH)

Tabulka č. 2

Úklid kanceláří	Systém školení			Režim návštěv	Bezpečnostní politika	
	Školení v budově OSZ	Školení organizované agenturou v jiných prostorách	Školení formou e-learningu		Zpracování vlastními zaměstnanci	Zpracování odbornou firmou
0,00- Kč	4.815,- Kč	12.959,00 Kč	2.356,00 Kč	0,00 Kč	0,00 Kč	166.000,00 Kč

Ušetřené náklady okresního státního zastupitelství za provedení analýzy rizik podle § 13 odst. 3 Zákona, kterou jsem zpracovala v této práci, se podle vlastního telefonicky provedeného průzkumu trhu pohybují v rozsahu **39.000,00 Kč až 56.000,00 Kč bez DPH (39.741,00 Kč až 66.640,00 Kč s DPH)**.

Přínos návrhů řešení

Řešení bezpečnosti s sebou nese nutnost řádně zpracovat bezpečnostní dokumentaci. Tvorba potřebných organizačních a technických dokumentů přináší množství úskalí, neboť každý z dokumentů pokrývá svou specifickou oblast, a přesto musí tvořit komplexní a srozumitelný systém. Funkční systém bezpečnostní dokumentace pokrývá oblasti od základních zásad a principů zajištění bezpečnosti, přes pracovní postupy až po technické detaily nastavení zařízení. Přínosem dokumentace je její efektivita a stanovení odpovědností, aniž by docházelo k překrývání informací v jednotlivých dokumentech a aniž by jejich údržba vyžadovala enormní zatížení zaměstnanců. Právě vhodnost a praktičnost formulování bezpečnostní politiky, na jejíž důležitost jsem poukázala, je **jedním z přínosů** mojí práce.

V průběhu sbírání podkladů a zpracování diplomové práce jsem úzce spolupracovala s vedením okresního státního zastupitelství, které přišlo s myšlenkou na využití této práce pro svou vnitřní potřebu. Vyhodnocením úrovně rizik, které je

součástí této práce, splnilo vedení OSZ ustanovení § 13 odst. 3 Zákona, a kdy na základě zjištěných nedostatků budou následně písemně zpracovány a do praxe zavedeny inovační procesy, resp. organizační opatření, která odstraní nedostatky popsané v této práci. Podle § 13 odst. 2 Zákona je totiž správce nebo zpracovatel povinen zpracovat a zdokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy. V tomto ohledu spatřuji **největší přínos** mé diplomové práce.

5 Závěr

Hlavním cílem mé diplomové práce bylo posoudit stav zavedených organizačních a technických opatření v oblasti zpracování osobních údajů u státní organizace. Dále pak posoudit a zdokumentovat možná rizika při manipulaci s nimi. Cílem bylo rovněž v návaznosti na zjištěné skutečnosti vypracovat návrh nezbytných inovačních procesů směřujících ke zvýšení bezpečnosti práce s osobními údaji, a to vše mělo vést k dosažení shody s platnou právní úpravou.

K dosažení cíle jsem dospěla jednak provedením analýzy stávajícího stavu okresního státního zastupitelství v procesu zpracování osobních údajů a jednak analýzou možných rizik, kdy jsem stanovila jejich velikost. Na základě zjištěné úrovně jednotlivých rizik, v kontextu se zjištěným stavem v procesu zpracování osobních údajů, jsem vypracovala několik návrhů na zavedení vhodných inovačních procesů, kterými lze dosáhnout větší bezpečnosti při jejich zpracovávání. Toto vše s cílem dosažení shody s platnou právní úpravou.

V teoretické části jsem se věnovala teoretickým východiskům diplomové práce ve vztahu k ochraně informací, charakteristikou vybrané organizace, ochranou osobních údajů, vybranými oblasti managementu a osobností manažera.

V praktické části práce jsem upřesnila metodiku a definovala požadavky § 13 Zákona na problematiku ochrany osobních údajů. Analýzu současného stavu v oblasti ochrany osobních údajů jsem prováděla podle jednotlivých oblastí, které jsem zvolila podle Standardu, a které byly relevantní k mnou zpracovávané problematice. V další části jsem zpracovala analýzu rizik, jejich vyhodnocení a dále pak výsledky analýzy a souhrn zjištěných nedostatků.

V závěru praktické části jsem uvedla návrhy řešení na zvýšení bezpečnosti při práci s osobními údaji a jejich přínos.

Diplomové práce ukazuje na obrovský rozsah a složitost celé problematiky týkající se oblasti zpracování osobních údajů. Záměrem práce bylo pokusit se najít rezervy a možnosti jak zlepšit stav při ochraně osobních údajů a pomocí zvolené metodiky dospět k návrhům, které zvýši jejich bezpečnost.

Na závěr chci upozornit na důležitost bezpečností politiky jako vrcholného a sjednocujícího dokumentu, který shrne veškeré bezpečnostní zásady a bude zdrojem odkazů na ostatní dokumenty. Vytvoření bezpečnostní politiky je zásadním

předpokladem pro zavedení řízení bezpečnosti informací, a tím i osobních údajů u okresního státního zastupitelství.

Záměrem této diplomové práce nebylo vyřešit problém ochrany osobních údajů komplexně, ale pokusit se navrhnout inovační procesy, které by zvýšily jejich bezpečnost. A to se na základě provedené analýzy, ze které vyplynula nutnost na zavedení nebo úpravu organizačních opatření, podařilo. V závěru lze tedy konstatovat, že cíle diplomové práce byly splněny.

Souhrn / Resumé

Diplomová práce se věnuje inovačním procesům zpracování osobních údajů u státní organizace. Provedenou analýzou stávajícího stavu opatření realizovaných na úseku ochrany osobních údajů a v kontextu s analýzou možných rizik, se podařilo najít rezervy a navrhnout možná řešení pro zlepšení stavu bezpečnosti osobních údajů. Práce ukázala na rozsáhlost celého problému, který překračuje její rámec, a na bezpečnostní politiku, jako na důležitý předpoklad účinnosti a efektivity bezpečnosti, nejen ochrany osobních údajů.

Thesis focuses on innovation processes personal data in state agencies. Analysis of state measures carried out in the field of protection of personal data in the context of the analysis of potential risks, managed to find reserves and to propose possible solutions for improving the state of security of personal data. Work has shown the extent of the problem, which goes beyond its framework, and security policy, as a prerequisite for effectiveness and efficiency of security, not only the protection of personal data.

6 Seznam použitých zdrojů

1. BARTES, F. *Inovace v podniku*. 1. vyd. Brno: AKADEMICKÉ NAKLADATELSTVÍ CERM®, s.r.o. 2005, 133 s. ISBN 80-214-3086-9.
2. BERKA, M. a kol. *Bezpečná počítačová síť.* Stav ke květnu 2006. (základní dílo včetně 8. aktualizace). Praha: Dashöfer Holding, Ltd. & Verlag Dashöfer nakladatelství, s.r.o. 2006, ISBN 80-86229-79-3.
3. BERKA, M. a kol. *Bezpečná počítačová síť.* Stav ke květnu 2006. (základní dílo včetně 9. aktualizace). Praha: Dashöfer Holding, Ltd. & Verlag Dashöfer nakladatelství, s.r.o. 2006, ISBN 80-86229-79-3.
4. BRABEC, F. a kol. *Bezpečnost pro firmu, úřad a občana.* Praha: Nakladatelství Public History, 2001.
5. CAHOVÁ, V. *Bezpečnostní analýza organizace.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2007. 49 s. Vedoucí bakalářské práce Ing. Jiří Kříž, Ph.D.
6. ČSN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2006.
7. ČSN ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2008.
8. DCIT, s.r.o. *Zpracování bezpečnostní dokumentace.* [online]. poslední aktualizace není uvedena [cit. 9. dubna 2009]. Dostupné na www: <http://www.dcit.cz/files/bezpecnost/info/DCIT_zpracovani_bezpecnostni_dokumentace.pdf>
9. DCIT, s.r.o. *Nezávislý důkaz vaší bezpečnosti.* [online]. poslední aktualizace není uvedena [cit. 9. dubna 2009]. Dostupné na www: <http://www.dcit.cz/files/bezpecnost/info/DCIT_posouzeni_shody_s_iso17799.pdf>

10. FRYŠAR, M. a kol. *Bezpečnost pro manažery, podnikatele a politiky*. Praha: Nakladatelství Public History ve spolupráci s českou asociací bezpečnostních manažerů, 2006, s. 9-18, s. 22-23, ISBN 80-86445-22-4.

11. HUMLOVÁ, A., SEIGE, V. *Vize informační bezpečnosti 2002/2003.* Praha: TATE International, s.r.o. 2006. 210 s. ISBN 80-902858-6-4.

12. KOCH, M. DOVRTĚL J. *Management informačních systémů.* 1. vyd. Brno: AKADEMICKÉ NAKLADATELSTVÍ CERM®, s.r.o. 2006, 174 s. ISBN 80-214-3262-4.

13. KOPEC, J. *Kontrolní systém společnosti jako součást procesu jejího řízení.* Praha: Český institut interních auditorů, 1999.

14. MEMORY, s.r.o.: *Ochrana osobních údajů*. [online]. poslední aktualizace není uvedena. [cit. 23. března 2009]. Dostupné na www: < http://www.oou.cz/index.php?file=ochrana_dat_proc_chranit_osobni_udaje>

15. NEJVYŠŠÍ STÁTNÍ ZASTUPITELSTVÍ ČESKÉ REPUBLIKY: *Úvodní slovo* [online]. poslední aktualizace 17. 2. 2009 [cit. 5. listopadu 2003]. Dostupný na www: <http://portal.justice.cz/justice/nsz./hlavni.aspx?j=39&o=29&k=2713&d=20274>

16. NĚMEČEK, P. ZICH, R. *Podnikový management 1. díl.* 2. vyd. Brno: AKADEMICKÉ NAKLADATELSTVÍ CERM®, s.r.o. 2006, 60 s. ISBN 80-214-3211-X.

17. NĚMEČEK, P. ZICH, R. *Podnikový management 2. díl.* 2. vyd. Brno: AKADEMICKÉ NAKLADATELSTVÍ CERM®, s.r.o. 2006, 90 s. ISBN 80-214-3212-8.

18. NĚMEČEK, P. ZICH, R. *Podnikový management 3. díl.* 1. vyd. Brno: AKADEMICKÉ NAKLADATELSTVÍ CERM®, s.r.o. 2005, 69 s. ISBN 80-214-3004-4.

19. PARLAMENT ČESKÉ REPUBLIKY. *Zákon č. 283/19933 Sb. o státním zastupitelství, ve znění pozdějších předpisů.* aspi-server kszbrnfs:6665. poslední aktualizace 10. 2. 2009 [cit. 12. února 2009].

20. RAIS, K. DOSKOČIL R. *Risk management.* 1. vyd. Brno: AKADEMICKÉ NAKLADATELSTVÍ CERM®, s.r.o. 2007, 152 s. ISBN 978-80-214-3510-0

21. STEINAR, F. [online]. poslední aktualizace 24. 3. 2009 [cit. 10. března 2008]. Dostupné na www: <http://home.zcu.cz/~steiner/ZPI/P%F8edn%E1%9Aka%203-4.pdf>

7 Seznam zkratek

Zákon	**Zákon č. 101/2000** Sb., o ochraně osobních údajů a o změně některých zákonů
OOÚ	ochrana osobních údajů
Standard	**ČSN ISO/IEC 17799** Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací
ISMS	**ČSN ISO/IEC 27001** Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – požadavky **ČSN ISO/IEC 17799** Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací
CIA	důvěrnost (Confidentiality), integrita (Intergrity), dostupnost (Availability)
KSZ	Krajské státní zastupitelství v Brně
OSZ	okresní státní zastupitelství
ISYZ	elektronické rejstříky trestních spisů
PO	právnická osoba
FO	fyzická osoba

8 Přílohy

Příloha č. 1: Organizační schéma okresního státního zastupitelství

Příloha č. 2: Žádost o umožnění zpracování diplomové práce