UNIVERZITA PALACKÉHO V OLOMOUCI

Pedagogická fakulta

Ústav pedagogiky a sociálních studií

BOHDAN VELIČKA

III. ročník – kombinované studium

Obor: pedagogika – sociální práce

MODERNÍ INFORMAČNÍ TECHNOLOGIE VE VEŘEJNÉ SPRÁVĚ

Bakalářská práce

Vedoucí práce: RNDr. Evžen Růžička, CSc.

OLOMOUC 2010

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a použil jen uvedenou literaturu a prameny.

V Olomouci dne 8. dubna 2010 ……

Bohdan Velička

Děkuji touto cestou RNDr. Evženu Růžičkovi, CSc. za odborné vedení bakalářské práce, cenné rady a připomínky, které mi poskytl.

OBSAH

ÚVOD..... 6

1 VZNIK A VÝVOJ INFORMATIKY…….....9

1.1 Vznik informačních technologií……....9

1.2 Informace…….10

1.3 Informační systém.……...11

1.4 Vznik internetu……12

1.4.1 Internet……..13

1.5 Současná situace informačních technologií…….14

2 VEŘEJNÁ SPRÁVA……...15

2.1 Struktura veřejné správy a dělení……15

2.2 Postup orgánů veřejné správy……..16

2.3 Výkon veřejné správy……..17

2.4 Základní registry……..……17

2.5 Moderní informační technologie veřejné správy…….18

2.5.1 Czech Point……...19

2.5.2 Datové schránky……...20

2.5.3 Elektronické soudní řízení ……...21

3 BEZPEČNOST INFORMAČNÍCH TECHNOLOGIÍ……...…23

3.1 Bezpečnost……..…….23

3.2 Aktuální hrozby pro informační bezpečnost……...23

3.3 Útoky na informační technologie……25

3.4 Ochrana uživatele……26

3.5 Bezpečnostní politika……..27

3.6. Legislativní rámec při práci s daty…….28

4 ANALÝZA SOUČASNÉHO VYUŽITÍ MODERNÍCH INFORMAČNÍCH TECHNOLOGIÍ V RÁMCI INSTITUCE MĚSTSKÉHO ŘEDITELSTVÍ POLICIE ČESKÉ REPUBLIKY…….....33

4.1 Policie ČR, popis a schéma…….33

4.2 Popis moderních informačních technologií v rámci instituce MŘ PČR…….35

4.2.1 Elektronické trestní řízení…….36

4.2.2 Kriminalisticky sledovaná událost……37

4.2.3 eSIAŘ……...43

4.2.4 Centrální evidence obyvatel…….44

4.2.5 Událost……..46

4.3 Současné moderní trendy informačních technologií aplikované v rámci instituce MŘ PČR……..……...47

4.4 Cíl rozvoje informačních technologií v instituci MŘ PČR…….48

4.5 Zhodnocení využívání informačních systémů v rámci instituce MŘ PČR a doporučení pro jejich kladný budoucí vývoj……..…50

ZÁVĚR…….53

SEZNAM LITERATURY A PRAMENY……..55

PŘÍLOHY

ANOTACE

1 Úvod

Komunikace od vzniku lidstva byla primární potřebou člověka, který pro své bytí potřeboval přijímat, předávat a také zpracovávat informace. Způsob předávaní těchto informací se s odstupem času vyvíjel. V současné době je člověk schopen předávat informace v rámci nových technologií na značnou vzdálenost. Současný trend je takový, že člověk je schopen tyto informace předávat prakticky všude. Také se velmi zjednodušil přístup k důležitým a potřebným informacím. Pokud jsou k tomu vhodné technické podmínky, tak předávání a využívání těchto informací je v podstatě bez omezení. Pracování s informacemi na značnou vzdálenost je už každodenní praxí a nutností. K tomu, aby to mohlo takto fungovat, tak se vyvíjejí informační technologie, které pomáhají člověku usnadňovat komunikaci. V práci s informacemi se nejčastěji používají počítačové systémy a jejich aplikace.

Veřejná správa je struktura institucí, které se podílejí na chodu státu v rámci své agendy. Instituce veřejné správy jsou ministerstva, kraje, obce a jím podřízené specializované instituce, které vykonávají potřebnou agendu pro chod státu. Tyto subjekty slouží státu účelně vykonávat správu ve věcech veřejných. Už z celkového názvu veřejná správa vyplývá, že tyto subjekty musí být uzpůsobeny, aby účelně komunikovaly s občanem a hlavně mezi sebou navzájem. Jejich informační technologie musí být zákonitě na vysoké technologické úrovni. Jako jedna z nejdůležitějších a nejúčelnějších oblastí ve veřejné správě je v současné době informatika. Informatika v sobě sdružuje informační systémy, které jsou dnes nezbytné pro řádný chod institucí. Jeden z významných komponentů informačních systémů ve veřejné správě jsou počítačově systémy vzájemně propojené počítačovou sítí. Ve veřejné správě jsou pro její účelný chod využívané různé aplikace datových zdrojů, převážně evidence osobních údajů, které se shromažďují pro pozdější využití. Současný trend je takový, že instituce je občanům blíže, komunikace se z osobní roviny přenáší do komunikace elektronické. Hlavně pomocí internetové sítě v rámci počítačových subjektů. Proto je velký důraz kladen na ochranu těchto údajů před zneužitím. Možnosti počítačově orientovaných informačních systémů sebou přinesly nejednu výhodu. Hlavní a nespornou výhodou je rychlost a přesnost předávané informace. Poslední dobou se počítačové aplikace velmi progresivně vyvíjejí a modernizují, kdy toto s přenosem do veřejné správy

přispělo k expanzi kvality služeb a nových přístupů k občanům. Přináší to nové možnosti oboustranné komunikace občanů s institucí veřejné správy, což přináší pro občana vetší možnost přístupu k informacím od institucí. Také to dává možnost lépe se orientovat ve veřejné správě. Veřejná správa je ve své podstatě nucena odbourat zbytečnou byrokratizaci, pracovat pomocí elektronických systému a používat nejmodernější informační technologie.

Tato bakalářská práce je zaměřena na stav moderních informačních technologií ve veřejné správě, zejména se zaměřením na informatiku a počítačové systémy. Cílem této práce je analýza moderních informačních systémů v konkrétní instituci ve veřejné správě, respektive v Policii České republiky a nastínění a navržení možnosti dalšího rozvoje těchto systémů.

Práce se rozděluje do jednotlivých kapitol podle svého obsahu a problematiky, ve kterých se rozpracovávají jednotlivé oblasti.

V první kapitole se pojednává o moderních informačních technologiích se zaměřením na informatiku. Popisuje se zde informační systém, jeho vznik, vývoj a použití.

Druhá kapitola je zaměřena na veřejnou správu, popis, účel těchto institucí a také na informační technologie, které se používají ve veřejné správě. Zde se uvádí rozbor aplikací a pracovních databází v informatice veřejné správy, které jsou používány na institucionální úrovni. Také se zde rozebírá situace nových trendů v elektronické komunikaci a uvádí se popis jednotlivých nově zavedených systémů v sektoru veřejné správy.

Ve třetí kapitole se řeší problematika bezpečnostní politiky v informatice se zaměřením na rizika při práci s daty a citlivými údaji osob. Je zde řešena právní stránka této oblasti a možnost zneužití osobních údajů. Také se zde zabýváme legislativním rámcem této oblasti.

Čtvrtá kapitola je empirická a je v ní uvedena analýza moderních informačních technologií na institucionální úrovni v rámci Městského ředitelství Policie České republiky v Ostravě. Zde je popis instituce, materiální zabezpečení a aplikace moderních informačních technologií v rámci této instituce. Cílem této práce bylo

vypracovat ucelený materiál, který může posloužit pro začínající pracovníky v oboru k lepší orientaci pří práci s informačními systémy. Práce je myšlena jako příručka využitelná v praxi.

Pro zpracování této práce byly čerpány informace z odborných knižních publikací, které se zabývají problematikou informačních technologií a problematikou veřejné správy. Z oblasti informačních technologií a veřejné správy byly také využity odborné časopisy, oficiální webové stránky, jednotlivé zákony, interní institucionální dokumenty a další relevantní zdroje.

1 **Vznik a vývoj informatiky**

1.1 Vznik informačních technologií

Informační technologie vznikají paralelně se vznikem Informační společnosti, tento název je zavedený v souvislosti s rozvojem a šířením nových, informačních a komunikačních technologií, které pracují s informacemi v datové, zvukové a audiovizuální formě směřující do všech oblastí ku prospěchu člověka. Tento termín se poprvé vyskytl ve zprávě Francouzské vlády někdy v roce 1975. Tato zpráva obohatila tradiční chápání telekomunikací i na otázky národní technologické suverenity a vytyčila vládní iniciativy včetně elektronického občanství. Informační společnost je charakterizována podstatným využíváním digitálního zpracování, uchovávání a přenosu informací. Tímto začíná nová epocha a ze zpracování informací vzniká ekonomická aktivita, která jednak postupuje tradičními ekonomickými či společenskými aktivitami a jednak vytváří zcela nové příležitosti a činnosti, které podstatně ovlivňují charakter společnosti. Primární technologickou základnou této proměny je využívání prvků moderních informačních technologií a digitálních komunikací. Dynamika pokroku v technologické konstrukci počítačových systému je již několik desetiletí motorem neomezeného růstu a neustálých inovací, což zatím není ničím omezeno a vývoj tohoto se progresivně zdokonaluje. Trendem je neustálá miniaturizace elektronických součásti těchto konstrukcí počítačových systémů a informačních technologií. Moderní informační technologie se také stávají dostupnější pro širší okruh uživatelů a už nejsou jen doménou vyspělých technických institucí. Základem informační technologie je mikroprocesor, který svou jednoduchostí se stal téměř všudypřítomnou součástkou a také cenově dostupným sortimentem. V současné době jsou čipy k nalezení prakticky všude, vyskytují se v automobilech, letadlech a dalších strojních zařízení, také usnadňují přepravu balíků v rámci zasílatelské služby. Čipy se vyskytují prakticky ve všech technických oblastech a samozřejmě se také vyskytují a jsou používány jako počítačové systémy. Informační technologie jsou hlavně o přenosu informací, kdy od analogového přenosu se v současné době převážně používá přenos informace v digitalizovaném tvaru. Takto zpracovaná informace je později použitelná ve všech oblastech a je univerzální, je duplikovatelná a transformovatelná. Ke zpracování jejího základu se využívá digitální

mikroprocesor, který umožňuje transformaci digitálního informačního záznamu a jeho kombinace s jinými. Informace, které byly dříve šířeny na papíře, rádiem, televizí, magnetickými páskami, mohou být v digitalizované podobě šířeny prostřednictvím jednoho multimediálního komunikačního kanálu. Informační a komunikační technologie umožnily vznik nové průmyslové revoluce s dopady, které mění způsob spolupráce ve společnosti. Mění život a nabízí nové možnosti uplatnění lidského potenciálu ve společenském zřízení. Vyhledávání, zpracování, uchovávání a předávání informací se stává nezávislé na časových, prostorových či kvantitativních omezeních. Budování informační společnosti se v různých podobách objevuje jako důležitá součást vládních programů všech rozvinutých zemí celého světa. Jedním z velkých impulzů v této oblasti bylo setkání zemí G7 v roce 1995, kde se dohodlo, že budování informační společnosti na mezinárodní úrovni je důležitý úkol.

1.2 Informace

Informace je souhrn sdělení prostřednictvím určitých znaků, které jsou příjemcem analyzované a aplikovatelné podle potřeby. *„Informace je článkem zpracovatelského řetězce (reálný svět – data – informace – znalosti). V tomto kontextu se data označují jako surovina pro přípravu informací. A informace společně s uloženými pravidly se stávají znalostmi. Použití výrazu informace ve významu zpráva, údaj, sdělení, poučení bylo rozšířeno až do padesátých let 20. století.*

Na každou informaci můžeme aplikovat tři různé úrovně pohledu v odpovídajícím uspořádání, v interpretaci a využití znaků:

- *Syntaxe, zabývá se vnitřní strukturou zprávy složené ze znaků dané abecedy, tj. zkoumá uspořádaní vztahů mezi znaky. Zároveň předpokládá analýzu informace nezávisle na jejím vztahu k objektu, který odráží. Tedy nezávisle na významu informace a na příjemci, který bude informaci využívat. Příkladem jsou pravidla pro zápis zprávy v konkrétním (přirozeném nebo umělém) jazyce.*

- *Sémantika, zajímá se o vztah k objektu, procesu nebo jevu, který tento znak odráží, nezávisle na příjemci. Příkladem je pochopení napsaného textu.*

- *Pragmatika, zkoumá vztah informace k příjemci, využití této informace, její praktický dopad na daný (např. ekonomický systém). Je to pro nás nejdůležitější, ale také neobtížnější formalizovatelná úroveň. Příklad: „praktický význam" zprávy pro osobu příjemce.*

Informace je tedy zpráva o nastalém jevu, která u nás příjemců snižuje míru neznalosti o tomto jevu." (Gála, L., Pour, J., Šedivá, Z., 2009, s. 22)

1.3 Informační systém

Souhrn různých subjektů, sloužících k předávání informací, využívajících různé technické komponenty moderní technologie. Na terminologii informačního systému existují různé definice. *„Informační systém lze definovat jako soubor lidí a metod a technických prostředků zajišťujících sběr, přenos, uchovávání, zpracování a prezentaci dat s cílem tvorby a poskytování informací dle potřeb příjemců informací činných v systémech řízení."* a v další z definic se praví *„Informační systém je obecně podpůrný systém pro systém řízení. Jestliže chceme projektovat systém řízení jako takový, musíme znát jaké jsou cíle, a informační systém řešit tak, aby tyto cíle podporoval."* (Tvrdíková, M., 2008, s. 18)

Informační systém lze rozčlenit podle těchto složek, které jsou nezbytné pro řádné a účelné fungování informačního systému:

- hardware, počítačové systémy různého druhu a velikosti,

- software, programové prostředky tvořené systémovými programy, řídící chod počítače, efektivní práci s daty a komunikaci počítačového systému s reálným světem, a programy aplikačními, řešícími určité třídy úloh určitých tříd uživatelů,

- orgware, organizační prostředky tvořené souborem nařízení a pravidel, definujících provozování a využívání informačního systému a informačních technologií,

- peopleware, lidská složka řešení otázky adaptace a účinného fungování člověka v počítačovém prostředí, do kterého je zařazen.

„Účelem informačního systému je zajištění vhodného vyjádření informací, jejich zpracování a přenášení v rámci nějakého systému. Obecně je pak tvořen lidmi, vhodnými nástroji a metodami, které jsou seskupeny do tří základních komponent:

- *vstup (input), zahrnuje prvky, umožňující zachytit informační a další vstupy, které mají být předmětem zpracování, případně vstupy vzájemně propojit,*

- *zpracování (processing), zahrnuje prvky, které zajišťují transformaci vstupů do požadovaného výstupu,*

- *výstup (output), představuje prvky, které jsou schopny přenést informační a další výstupy k jeho příjemci (uživateli).“* (Gála, L., Pour, J., Šedivá, Z., 2009, s. 23)

1.4 Vznik internetu

Stěžejním impulsem ve vývoji informačních technologií byl projekt vzniku ARPANETU. V roce 1957 v rámci Amerického ministerstva obrany založila vláda Úřad pro pokročilé výzkumné projekty. Tento úřad vznikl hlavně proto, že vláda si chtěla zajistit prvenství ve vědě a technologiích ve vojenství. V tomto projektu se zabývali hlavní myšlenkou decentralizace počítačové sítě, aby v tomto systému nebyl ani jeden kritický bod, aby nemohl být zničitelný jediným jaderným útokem. Projekt se poté nazval ARPANET. Po deseti letech byla vyvinuta fungující síť a tímto byly v roce 1969 položeny základy revoluce v informačních technologiích, která se stále vyvíjí a zažíváme ji na každém kroku. Tímto tedy začal vznik internetu v technické rovině, jelikož ještě dlouhou dobu trvalo než se internet začal používat masově i pro občanské účely. Zpočátku byla tato síť využívaná armádou a vědeckými pracovišti. Postupně s rozvojem dalších sítí, které bylo možno propojovat vzniky i nové možnosti využití těchto sítí. Jednou z prvních funkcí sítí

bylo posílání a přijímání počítačových souborů a elektronické pošty. Tyto technické inovace byly technický náročné a zpočátku se vyvíjely jen ve vyspělých zemích. Zpočátku byla rychlost přenosu dat po těchto sítích velmi malá a s odstupem času rostla. V roce 1986 byla rychlost přenosu na hlavní síti až 56 kilobitů za sekundu, kdy k tomuto bylo zapotřebí pět superpočítačových středisek. Následně došlo k revoluční explozi počítačů nově připojených do internetu. Rychlost přenosu datových informací se výrazně zvýšila. Vznikají nové internetové služby. Objevuje se první komerční poskytovatel přístupu Internetu. K internetu se postupně připojovaly další země a společnosti. Česká republika se k internetu připojila v průběhu roku 1992 a v tento rok došlo i k založení společnosti zabývající se historií, vývojem, trendy a etikou internetu. Počet zúčastněných počítačů v síti překročil jeden milión. Roku 1993 se zakládá instituce k udržování adresářové a databázové služby účastníků internetu, která provádí registraci doménových jmen a přidělování adres. Internet se stal masovým médiem a prostřednictvím této sítě můžeme čerpat informace všeho druhu, jeho možnosti jsou prakticky neomezené. Na internet jsou připojené různé instituce, jak ze soukromého sektoru, tak ze sektoru veřejného. Internet se stává součástí běžného života. Zejména se používá elektronická pošta. Internet svou masovostí docílil toho, že se stává přístupnější všem. Internet je používán hlavně pro využívání a předávání informací, rozvijí se interaktivní práce uživatele s tímto médiem. Internetová síť slouží ke komunikaci a k předávání upotřebitelných informací. Instituce veřejné správy i jako jiné instituce byly nuceny začít využívat služeb, které nabízí Internet a elektronická komunikace.

1.4.1 Internet

Internet je počítačová síť, která pomocí nástrojů ICT (informačních a komunikačních technologií) umožňuje vyhledávání a sdílení údajů a informací, tzv. dálkový přístup k informacím. Počítačové sítě internetu se nazývají www. Internet je velmi důležitý nástroj na podporu eDemokracie a participace, zabezpečující podíl veřejnosti na rozhodovacích procesech veřejné správy. Samozřejmě je také nástrojem pro vytváření různých sociálních sítí a slouží pro účely soukromé, obchodní a veřejné. *„V době, kdy nebyl internet k dispozici a ani*

lokální sítě nebyly příliš rozšířeným prostředím, byl přenos informací mezi systémy realizován zpravidla pomocí různých záznamových médií, možnost dvou a více aplikací se neuvažovala – případný přenos dat probíhal zpravidla pomocí zmíněných záznamových médií, což bylo časově velmi náročné.“ (Bureš, M., Jelínek, I., Morávek, 2005, s. 33)

1.5 Současná situace informačních technologií

V současné době je situace taková, že informační technologie, informatika a elektronizace jsou názvy, které nás potkávají na každém kroku. Informační technologie jsou všudy přítomné. Počítačový systém je nezbytným pomocníkem při řešení pracovních i osobních problémů. Lidstvo využívá těchto moderních technologií naplno a technologie svou masovostí se stávají dostupné pro všechny. Informatika jako taková je nezbytnou součásti každého života. V minulosti, když člověk potřeboval nějaké konkrétní informace, musel si najít pramen těchto informací a pak musel tento pramen prostudovat a potřebné informace si vybrat. V současnosti tento pramen máme většina z nás doma a tímto pramenem je počítačový systém s připojením na internet. Do tohoto systému zadáme analogii potřebnou k vyhledání informace a internet nám nabídne několik možností k využití z několika zdrojů k čerpání. Pak stačí potřebnou informaci vybrat a uložit si ji pro svou potřebu. Když jsme v minulosti shromažďovali nějaké potřebné informace pro pozdější využití, tak jsme si museli pořídit archív k uskladnění těchto potištěných papírů. Dnes stačí informace uložit na určitý druh média, které je skladné. Dnešní doba je tedy velmi technická, informace se dají čerpat ve větším měřítku, rychle a z různých zdrojů. Tento čas, který jsme takto ušetřili, můžeme poté využívat v jiných oblastech našeho života. Současná situace je taková, že bez počítačového systému a připojení na internet se člověk neobejde. Tomuto trendu se musí přizpůsobit každý. Moderní informační technologie jsou masově přístupné všem, jsou nutností a usnadňuji lidem život. Tento současný trend není jenom o kladech, ale přináší sebou i možné problémy a patologie. Zde se dá hovořit o kyberšikaně, podvodech, krádežích osobních údajů a dalších negativních jevech. I přes tyto uvedené zápory, jsou klady přínosů moderních informačních technologií pro veřejnost a instituce, stále velkým přínosem.

2 Veřejná správa

2.1 Struktura veřejné správy a dělení

Veřejná správa je určitý druh činnosti sledující spravování veřejných záležitostí prostřednictvím institucí, které veřejnou správu vykonávají.

V materiálním pojetí je veřejná správa činností státních nebo jiných veřejných institucí, která svým obsahem není ani činností zákonodárnou, ani soudní. Ve formování v rámci institucionálního organizačního pojetí je veřejná správa definovaná jako činnost orgánů označených jako správní úřady. Pojem veřejná správa je termínem společným a nadřazeným pro pojem státní správa, která je vykonávána především státními orgány, samospráva, která je vykonávanýma orgány územních samosprávných celků či orgánu zájmové, profesní samosprávy a ostatní veřejná správa, která je vykonávaná zejména institucemi s právní subjektivitou. Zde můžeme hovořit např. o VZP, ČNB, ČT, ČTK (Všeobecná zdravotní pojišťovna, Česká národní banka, Česká televize, Česká tisková kancelář). Takto o veřejné správě hovoří D. Hendrych (2009) autor obecné části Správního práva.

Veřejná správa se dělí na dva subsystémy:

- státní správa,

- samospráva.

Státní správa, už jak ze svého názvu vyplývá je soubor institucí, prostřednictvím kterých stát uplatňuje státní moc. Státní správa je zařazena mezi orgány výkonné činnosti státu. *„Státní správa je především činností podzákonnou, prováděcí a nařizovací. Subjekty státní správy je stát, orgány státní správy, které vykonávají veškerou aktivitu jménem státu, dále pak veřejnoprávní korporace, jejich orgány a jiné subjekty, jímž byl výkon státní správy svěřen.“* (Halásková, M., 2006, s. 8)

Samospráva, výkon provádí někdo jiný než stát. Samospráva nepodléhá státní správě, ale činí s ní komplementární dvojici, která se navzájem doplňuje, ale přičemž mohou někdy stát i proti sobě (např. v soudním sporu). Moderní systémy

samosprávy jsou založeny na principu subsidiarity, tzn. přenesení rozhodovací pravomoci na úroveň nejbližší vlastnímu procesu. Základní členění samosprávy je na územní a zájmovou. Územní samospráva tvoří spolu s místními orgány státu tzv. místní veřejnou správu a krajskou veřejnou správu. Je tedy představována obcemi, resp. městy jako základními články samosprávy a vyššími územně správními celky – kraji (Vyššími územně samosprávnými celky jsou Středočeský kraj, Jihočeský kraj, Plzeňský kraj, Karlovarský kraj, Ústecký kraj, Liberecký kraj, Královehradecký kraj, Pardubický kraj, kraj Vysočina, Moravskoslezský kraj, Olomoucký kraj, Zlínský kraj, Jihomoravský kraj a hlavní město Praha). Zájmová samospráva se především týká určitého druhu osob a sdružení, jako např. advokátů, lékárníků, lékařů, studentů vysokých škol a dalších. Obecný výkon veřejné správy představují orgány veřejné správy, mezi které patří ministerstva, jiné správní úřady, orgány územní samosprávy a další instituce.

2.2 Postup orgánů veřejné správy.

V zákoně č. 500/2004 Sb., správní řád je upraven postup orgánů moci, orgánů územních samosprávných celků a jiných orgánů, právnických a fyzických osob, pokud vykonávají působnost v oblasti veřejné správy. (§ 1 odst. 1 zákona č. 500/2004 Sb., správní řád) a dále se zde praví, v ust. § 4 odst. 1, že veřejná správa je službou veřejnosti. Každý, kdo plní úkoly vyplývající z působnosti správního orgánu, má povinnost se k dotčeným osobám chovat zdvořile a podle možnosti jim vycházet vstříc. V ust. § 6 odst. 1, odst. 2 tohoto zákona se praví, že:

Ad. 1 Správní orgán vyřizuje věci bez zbytečných průtahů. Nečiní-li správní orgán úkoly v zákonem stanovené lhůtě nebo ve lhůtě přiměřené, není-li zákonná lhůta stanovena, použije se ke zjednání nápravy ustanovení o ochraně před nečinností.

Ad. 2 Správní orgán postupuje tak, aby nikomu nevznikaly zbytečné náklady, a dotčené osoby co možná nejméně zatěžuje. Podklady od dotčené osoby vyžaduje jen tehdy, stanoví-li tak právní předpis. Lze-li však potřebné údaje získat z úřední evidence, kterou správní orgán sám vede, a pokud o to dotčená osoba požádá, je povinen jejich obstarání zajistit. Při opatřování údajů podle tohoto ustanovení má

správní orgán vůči třetím osobám, jichž se tyto údaje mohou týkat, stejné postavení jako dotčená osoba, na jejíž požádání údaje opatřuje.

2.3 Výkon veřejné správy

Veřejná správa je správa věcí veřejných záležitostí, která je realizována především jako výkonná moc. Výkon veřejné správy je činnosti podzákonnou, neboť orgány veřejné správy jsou vázány zákony a dalšími právním předpisy nižší právní síly i vyšší právní síly. Výkon veřejné správy je chápán jako veřejná služba. Na výkonu veřejné správy se podílí stát prostřednictvím státních orgánů a veřejnoprávní korporace – orgány územních samosprávných celků a orgány zájmové samosprávy, kterými jsou svazky, profesní komory a podobně. Takto se o tomto hovoří v zákoně č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonů veřejné moci.

Z těchto zákonných ustanovení je zřejmé, že veřejná správa jako taková má sloužit ku prospěchu občanů a má jim ulehčovat styk s úřady. K tomuto, aby toto mohlo fungovat musí být instituce veřejné správy vybaveny příslušným informačním zázemím, jelikož v současné době je zcela nezbytné být vybaven informatikou a využívat různé druhy registru informací. Každá instituce ve veřejné správě, potřebuje pro svůj produktivní chod informační technologie k využívání potřebných informací. Rychlý a snadný přístup k informacím je nutností a proto jsou zřízeny různé databáze s registry informací ke sdílení dat, které jsou přístupné oprávněným subjektů.

2.4 Základní registry veřejné správy

Základní registry jsou komponovány v informačním systému veřejné správy, který obsahuje referenční údaje a primárně slouží pro rozšiřování služeb pro občany v rámci strategie rozvoje projektu eGovernmentu, což je souhrnný název pro postup modernizace veřejné správy s využitím nových možností informačních a komunikačních technologií. Tyto registry představují soubory dat a údajů, které

bude sdílet celá veřejná správa. Ostatní registry budou čerpat údaje ze základních registrů, které se dělí:

- územní identifikace a nemovitostí,
- obyvatel,
- osob,
- práv a povinností.

Dále se můžou tyto registry dělit podle kriterií potřebnosti, funkčnosti a působnosti a další dělení lze užít v rámci institucí samých.

Ke správě těchto registrů celého informačního systému veřejné správy je pověřen správce a k provozu provozovatel.

Provozovatelem je subjekt, který provádí dílčí úkoly příslušného informačního systému. Provozovat informační systém veřejné správy, lze na základě pověření správce, pokud to zákon nevylučuje.

Správce informačního systému *„je subjekt, který podle zákona č. 365/2000 Sb. určuje účel a prostředky zpracování informací a za informační systém odpovídá.*

Správci informačních systému veřejné správy jsou:

- *ministerstva,*
- *orgány územní samosprávy,*
- *jiné správní orgány,*
- *další státní orgány.“* (Halásková, M., 2006, s. 76)

2.5 Moderní informační systémy veřejné správy

Moderní informační systémy veřejné správy jsou o tom, že veřejná správa se blíží více k občanům samotným a usnadňuje jim komunikaci s úřady. Pro občany se

stává úřad dostupný elektronickou formou a odbourává se zbytečná byrokracie. Občanům modernizace usnadňuje život. V této sféře modernizace můžeme jmenovat tři příklady zavádění moderních informačních technologií do veřejné správy.

Jedná se o:

- Czech point.
- Datové schránky.
- Elektronické soudní řízení.

2.5.1 Czech point

Český Podací Ověřovací Informační Národní Terminál, tedy Czech POINT je projektem, jehož cílem je zredukovat přílišnou byrokracii ve vztahu občan – veřejná správa. V současnosti musí občan často navštívit několik úřadů k vyřízení jednoho problému. Czech POINT slouží jako asistované místo výkonu veřejné správy, umožňující komunikaci se státem prostřednictvím jednoho místa tak, aby obíhala data a ne občan.

Cílem projektu Czech POINT je vytvořit garantovanou službu pro komunikaci se státem prostřednictvím jednoho universálního místa, kde je možné získat a ověřit data z veřejných i neveřejných informačních systémů, úředně ověřit dokumenty a listiny, převést písemné dokumenty do elektronické podoby a naopak, získat informace o průběhu správních řízení ve vztahu k občanovi a podat podání pro zahájení řízení správních orgánů. Jde tedy o maximální využití údajů ve vlastnictví státu tak, aby byly minimalizovány požadavky na občany.

Projekt Czech POINT přináší značné ulehčení komunikace se státem. V některých situacích stačí dojít pouze na jeden úřad. V konečné fázi projektu by občan mohl své záležitosti vyřizovat i z domova prostřednictvím internetu.

Jedná se o tyto oblasti:

- Výpis z Katastru nemovitostí.
- Výpis z Obchodního rejstříku.
- Výpis z Živnostenského rejstříku.
- Výpis z rejstříku trestů.
- Přijetí podání podle živnostenského zákona (§ 72).
- Výpis z bodového hodnocení řidiče.
- Vydání ověřeného výstupu ze Seznamu kvalifikovaných dodavatelů.
- Podání do registru účastníků provozu modulu autogramů ISOH.
- Výpis z insolventního rejstříku.
- Datové schránky.
- Autorizovaná konverze dokumentů.
- Centrální uložiště ověřovacích doložek.
- Úschovna systému Czech POINT.
- CzechPOINT@office.
- Czech POINT E-SHOP – výpisy poštou.

Výpisy získané prostřednictvím místa Czech POINT jsou primárně určeny k využití na území České republiky. V zahraničí lze listiny použít podle zvláštních pravidel a je nutné listinu získat u vlastníka agendy vydávající předmětnou listinu.

2.5.2 Datové schránky

Pro informační systém datových schránek je dán legislativní rámec v zákoně č. 300/2008 Sb. ISDS (Informační systém datových schránek) je zde jako jeden z klíčových pilířů HEXAGONU, což je vytváření principů SmartAdministration.

V České republice se opírá v eGovernmentu o informační systém základních registrů, o informační systém datových schránek, o kontaktní místa veřejné správy a o jednotnou infrastrukturu. ISDS je rychlé předávání potřebných informací v rámci veřejného sektoru. Datová schránka je elektronické uložiště nebo-li datový prostor, který je určen k doručování orgány veřejné moci a k provádění úkonů orgánům veřejné moci a také je to elektronické uložiště, které slouží k dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob. Zřízení a správu datových schránek provádí Ministerstvo vnitra. ISDS je informačním systémem veřejné správy ve smyslu zákona č. 365/2000 Sb., a je primárně učen k doručování dokumentů mezi orgány veřejné moci navzájem a také mezi orgány veřejné moci a právnickými osobami. ISDS je také k využití pro fyzické osoby. ISDS nabízí určitou podobnost s e-mailovou schránkou, ale ve své podstatě je do úplně jiný systém s neomezenou kapacitou a v žádném případě se nejedná o e-mailový server. ISDS je informačním systémem veřejné správy, který obsahuje informace o datových schránkách a jeho uživatelích. Jeho zřízení, provoz, ochrana uložených osobních údajů, ochrana přepravovaných informací se řídí právními předpisy. Ochrana osobních údajů a přepravovaných zpráv je zaručena tím, že na vstupu datové zprávy do systému je tato zašifrována a je rozšifrována až na výstupu. ISDS jako takový nevede a také nemůže vést žádný záznam o obsahu komunikace.

2.5.3 Elektronické soudní řízení

Elektronické soudní řízení se rozvíjí jak v oblasti občanského práva, tak v oblasti trestního práva. V obou těchto oblastech má elektronizace svá specifika a je implementována různými způsoby. Hlavní princip je stejný a jde o elektronizaci těchto soudních systémů, aby byly komplexně a účelně využívány výdobytky moderní informatiky. V rámci Evropské unie je koncipována řada projektů směřujících do elektronického soudnictví. V České republice se zavádí elektronické soudní řízení a připravuje se platná legislativa. Elektronické soudní řízení by mělo za následek podstatné snížení nákladů na materiální zabezpečení dotčených institucí, výrazně by přispělo ke zrychlení soudního procesu a zvýšilo by pružnost a efektivitu soudu. Sebou také přináší zvýšení počátečních nákladů při realizaci

tohoto projektu a poté náklady na řádně zabezpečení využívaných a shromažďovaných informací. Nezbytnou součásti elektronického soudního řízení je elektronický soudní spis (tzv. eSpis). V oblasti trestního práva vznik takových spisů znamená pro orgány činné v trestním řízení, snadnější a levnější komunikaci a to jak vnitroresortní tak mimoresortní. Jednou z velkých výhod je úspora práce při pořizování vstupních dat. Vzhledem k unifikaci je tento proces transparentní. Dalším kladem je dobrá kontrolovatelnost práce na těchto spisech, což zabraňuje průtahům a zvyšuje produktivitu a rychlost zpracování jednotlivých věcí. V rámci celé České republiky je možné komunikovat elektronickou formou při práci na těchto spisech a je možné pracovat na těchto spisech z jakého-koliv místa, ne jenom z lokálního působiště. Ve spisech může najednou pracovat větší množství osob, které jsou k tomu oprávněny.

3 Bezpečnost informačních technologií

V této kapitole se budeme komplexně zabývat bezpečnosti informačních systémů, hlavně podle jeho jednotlivých komponentů, hardwaru, softwaru, peoplewaru, dat i vlivů reálného světa.

3.1 Bezpečnost.

Bezpečnost v informatice je jedním ze základních problémů při aplikaci informačních technologií a systémů. *„Bezpečnost informačního systému je důležitou součásti jeho koncepce a vývoje. Význam kvalitního zabezpečení informačních systémů stále roste. Bylo by však chybné zužovat tento problém pouze na problematiku ošetření bezpečnosti informačních technologií, neboť informační technologie jsou pouze jednou z části informačních systémů. Je nezbytné nahlížet na bezpečnost komplexně a snažit se o zabezpečení informačního systému dané firmy nebo instituce ve všech jeho částech a na všech jeho rozhraních. Mezinárodní průzkumy avizují trend nárůstu hrozeb pro informační bezpečnost. Budování a provozování systému řízení informační bezpečnosti – ISMS (Information Security Management Systém) je jedinou možnou cestou, jak zajistit bezpečnost informací ve firmě či instituci.“* (Tvrdíková, M., 2008, s. 155)

3.2 Aktuální hrozby pro informační bezpečnost

V důsledku toho, jak se prostřednictvím informatiky, moderních informačních systémů a technologií přibližujeme ke koncovému uživateli. Tímto také narůstá riziko napadení shromažďovaných dat a zneužití těchto údajů. Analýzou tohoto problémů se zabývá celá řada společností, které reagují na tento problém vyvíjením celé řady zabezpečovacích prvků a doporučení. Hlavní bezpečnostní riziko informačních systémů je napadení tohoto systému neoprávněným uživatelem, jehož cílem je kopírovat citlivé údaje a tyto poté zneužít. Instituce veřejné správy jako takové pracuji s různými citlivými údaji, které shromažďují ve svých registrech a tyto údaje mnohdy obsahují komplexní identifikační údaje k fyzickým osobám, právnickým osobám, movitým i nemovitým věcem. V dnešním příliš

elektrizovaném světě jsou tyto údaje snadno zneužitelné a bránit proti tomuto zneužití se lze jen velmi těžko.

Aktuálním hrozbami v informační bezpečnosti jsou:

- webové stránky zaměřené na krádež hesel,
- spamy (zejména obrázkový, jsou nevyžádána sdělení masově šířené internetem, nejčastěji reklamní),
- škodlivý kód malware (malware je počítačový program určený ke vniknutí do počítačového systému a jeho poškození, tento výraz vznikl složením anglických slov „malicious“ (zákeřný) a „software“. Pod označení malware se zahrnují počítačové viry, trojští koně),
- spyware (je to program, který využívá internetu k odeslání dat z počítače bez vědomí uživatele),
- adware (znepříjemňuje práci s nějakou aplikací),
- útok na mobilní zařízení,
- krádež identity,
- užívání počítačových programů provádějících automatické útoky (tzv. boty, které jsou automatické programy působící přes webové rozhraní),
- rootkity (rootkit je sada počítačových programů a technologií, pomocí kterých lze maskovat přítomnost zákeřného softwaru v počítači).

„Společnost Ernst&Young zpracovala v roce 2006 průzkum stavu informační bezpečnosti (Global Information Security Survey), ze které vyplynulo, že technologiemi, kterým je v současné době zapotřebí věnovat největší pozornost z hlediska zajištění bezpečnosti jsou:

- *Technologie přenosných médií.*

- *Mobilní výpočetní technika PDA (personal digital assistant je počítač do ruky), smartphones (chytré telefony, komunikátory). Od klasických mobilních telefonů se liší nejen vzhledem, ale hlavně softwarovým vybavením, větší paměti (s možností rozšíření pomocí pamětových karet), větším displejem apod. Smart telefony mají obdobné funkce i využití jako klasické PDA.*

- *Bezdrátové sítě.*

- *Webové aplikace."* (Tvrdíková, M., 2008, s. 156)

3.3 Útoky na informační technologie

Jsou nežádoucím úkazem moderní technické doby, kdy vznikají z nejrůznějších důvodů. Úroveň zranitelnosti informačních systémů se hodnotí podle jeho citlivosti, náchylnosti aktiva a kritičnosti aktiva. Zranitelné místo je hrozbou informačního systému, kterou lze charakterizovat jako možnost využít zranitelné místo aktiva k útoku na toto aktivum. Útoky jsou označované jako bezpečnostní incident (security incident). Bezpečnostní incident lze charakterizovat jako skutečnost, která vede k porušení nebo prolomení nastavených bezpečnostních parametrů informačního systému. Hrozby a zranitelné místa využívají útočníci k vedení svého útoku. Útočníkem může být osoba uvnitř organizace nebo může jít osobu mimo organizaci. Útok může mít jasný úmysl nebo se jedná o neúmyslný útok. V případě osob, které realizují úmyslné útoky, se používá pro jejich označení několik termínů, zejména:

- hacker, bere útok jako výzvu a prostředek získání prestiže,

- vyzvědač (spy), provádí útoky za účelem zisku informací, které jsou využívány pro různé politické účely,

- terorista (terrorist), provádí útoky za účelem vyvolání a strachu,

- kriminálník (criminal), útočí na systémy pro svůj osobní finanční zisk,

- vandal, útočí na systémy s cílem systém zničit či poškodit,

- cracker, zpravidla programátor, který se snaží proniknout do systémů jiných vlastníků za účelem jejich krádeže, typicky se orientuje na krádež duševního vlastnictví, tj. těch součásti systémů, které jsou chráněny autorským zákonem,

- phracker, jeho cílem je získání bezplatného přístupu k telefonním službám,

- phreaker, jeho cílem jsou telekomunikační informace, které mu umožňují získávat přístup k dalším počítačům.

Hrozby a zranitelná místa tedy zvyšují riziko bezpečnostního incidentu. Riziko vyjadřuje míru ohrožení aktiva, míru nebezpečí, že se uplatní hrozba a dojede k nežádoucímu výsledku vedoucímu ke vzniku škody. Uvedené rozdělení uvádí L. Gála, J. Pour a Z. Šedivá (2009) ve své knize „Podniková informatika“.

3.4 Ochrana uživatele

Ochrana uživatele informačních technologií v moderním světě, zejména počítačových systémů přispívá k řádnému fungování těchto systémů a k bezpečnosti přenášených dat. Je uváděno pět složek ideálního systému pro identitu, bezpečnost a soukromí jednotlivců v informačních systémech. Jsou to autentizace, autorizace, soukromí, integrita a neodvolatelnost.

Mezi technologické prostředky ochrany uživatele patří zejména:

- antivirové programy kontrolující uložené a zpracované soubory na přítomnost virů,

- firewal sledující nejen příchozí, ale také odcházející komunikaci, tj. prostředek sledující, jaké zprávy ze systému odcházejí a kam, protože jejich abnormální počet může signalizovat přítomnost škodlivého kódu,

- anti-spyware programy sledující škodlivý kód (spyware) v programech, které se jako viry neprojevují,

- pravidelná aktualizace chyb vadnými záplatami u již instalovaného programového vybavení.

Mezi současné prostředky v oblasti antivirových programů patří ESET NOD32 Antivirus, Norton Antiviru, AVG, Avast, Kaspersky Antivirus, McAfee Antivirus. Dále v oblasti eliminace spyware jsou to třeba Spybot Search&Sestrou, Spyware Terminátor, AD-Aware a další. Tyto programové vybavení jsou uživateli poskytovaný jako placená služba s pravidelnou aktualizací tohoto programu a dobré antivirové vybavení počítačového systému může zachránit cenná data a je nezbytností. Některé antivirové programy jsou také bezplatné, volně ke stažení prostřednictvím internetu na příslušných stránkách, ale jen pro soukromé využití. Dalším z významných opatření uživatele proti ztrátě dat jsou uložiště dat. Do těchto systémů jsou data pravidelně ukládána, aby nedošlo k jejich ztrátě při nenadále situaci v rámci informačního systému. Potřebná data jsou ukládána centrálně, mimo individuální počítačový systém a jsou několikrát jištěna proti ztrátě. Ve zjednodušené formě se jedná o archív, kde se vše archivuje a data se z něj čerpají jen v případě potřeby. Ochrana uživatele je tedy velmi potřebná a každá instituce musí tomuto problému věnovat zvýšenou pozornost.

3.5 Bezpečnostní politika

Bezpečnostní politika je soubor pravidel a zásad, které ve vzájemném kontextu vedou ke snížení rizik neoprávněného napadení informačního systému a chrání uživatele před zneužitím využívaných dat. Bezpečnostní politika vychází ze studie informační bezpečnosti dané instituce, analýzy rizik a poté musí pružně reagovat na nově vzniklá rizika v rámci informatiky a musí aktivně přistupovat k řešení vzniklých problémů.

Bezpečnostní politiku lze dělit na tyto části podle bezpečnosti:

- fyzická,

- personální,

- bezpečnost informačních technologií,

- bezpečnost administrativní a procedurální.

„Po realizaci bezpečnostních mechanizmů na základě bezpečnostní politiky je potřebné monitorovat, zda jsou v dané době stále funkční. Vzhledem k rafinovanosti a vývoji útoku na informační systémy lze doporučit zadání této činnosti externí firmě, jejíž zaměstnanci jsou na problém soustředěni a mají v této oblasti speciální znalosti.“ (Tvrdíková, M., 2008, s. 156)

V rámci konkrétních institucí je potřeba vyhodnotit rizika možných hrozeb informačního systému individuálně a následně reagovat na konkrétní problémy. Je třeba rizika vyhodnocovat v pravidelných intervalech a reagovat na nové trendy hrozeb pro informační systémy. Ochrana těchto systémů není jednorázovou záležitostí, ale je to soustavná pravidelná činnost. Je potřeba klást zvýšený důraz na to s jakými daty pracuji a podle toho zlepšit či zmírnit ochranu systému. Počítačový systém jako takový je nejvíce zranitelný prostřednictvím počítačové sítě a pokud tento počítačový systém nepotřebuje využívat dat prostřednictvím této sítě, tak jej do sítě nelze zapojit. Mnohdy jednoduchá řešení problémů jsou ta nejúčinnější.

Bezpečnostní politika musí směřovat k modernizaci bezpečnostních systémů, jejich zabezpečení a vybavení bezpečnostními prvky a paralelně také k soustavnému proškolování bezpečnostních rizik samotných zaměstnanců, tedy koncových uživatelů informačních systémů. Lidský faktor je v tomto problému neopomenutelný, kdy jako jedno z velkých bezpečnostních rizik jsou zaměstnanci sami. I dobře zabezpečený systém může být napaden a poškozen zaměstnancem samým, který o tom mnohdy ani neví, že způsobil problémy. Počítačové systémy by měly být v rámci samotných institucí používány jen pro takový účel, pro který jsou určeny. Uživatel tohoto systému by zase neměl mít přístup ke všem aplikacím, ale jen k těm, které skutečně potřebuje pro svou činnost. Vstup do těchto aplikaci by neměl být samozřejmostí, ale mělo by být vše chráněno přihlašovacím heslem, které by mělo splňovat určité parametry Mělo by mít bezpečnou skladbu znaků, což znamená určitou strukturu a pořadí znaků. Čím více různých znaků, tím je heslo bezpečnější. V počítačových systémech by také měly být nainstalovány jen ty aplikace, které jsou potřebné pro chod toho konkrétního systému. Dále je také nutné dodržovat určité nařízení a postupy týkající se zasílání a přijímání nepovolených typů příloh, stahování jakýchkoliv neznámých aplikací nebo samospustitelných souborů, navštěvování nepovolených či rizikových WWW stránek a podobně.

K tomuto nám může pomoci zařízení, které se jmenuje Firewall či proxyserver. Což je síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovni důvěryhodnosti a zabezpečení. V podstatě jde o kontrolu komunikace mezi sítěmi, které od sebe odděluje. Proxyserver funguje jako prostředník mezi klientem a cílovým serverem, odděluje lokální počítačovou síť od internetu. Správné nastavení firewallu či pravidel proxyserveru může nežádoucí rizikové chování uživatelů výrazně omezit, ale nikdy je nemůže vyloučit úplně. Tedy ani technické vymoženosti nezbavují uživatele, aby sám měl dodržovat základní pravidla bezpečnosti. K eliminaci rizik je důležitý výběr a aplikace vhodných technických opatření. *„Tím můžeme rozumět např. zavedení přístupových karet, omezení práv přístupu uživatelů k datům podle jejich skutečných potřeb a stupně důležitosti dat, nastavení práv uživatelů komunikujících prostřednictvím internetu, protivirovou kontrolu veškeré komunikace směřující dovnitř i ven z vnitřní sítě a podobně. Zajištění technické části bezpečnosti lze dosáhnout pomoci správného nastavení firewallů, volbou vhodné vnitřní architektury sítě a dalšími způsoby. Při posuzování bezpečnosti je třeba si uvědomit, že každý systém je silný jen tak, jak silný je jeho neslabší článek. V případě zabezpečení informačních systému je nejslabším článkem jednoznačně uživatel.“* (Tvrdíková, M., 2008, s. 165)

Bezpečnostní politika je v podstatě samostatný a nezbytný obor v rámci konkrétních institucí, aby byl zajištěn bezproblémový chod informačních technologií, potažmo počítačových systémů a aplikací.

3.6 Legislativní rámec při práci s daty

Legislativa v rámci bezpečnosti při práci s informačními systémy a shromažďováním dat je v neustálém vývoji a musí pružně reagovat na nově vzniklé problémy, kdy mezi důležité zákonná ustanovení v rámci této oblasti patří:

- zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů,
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti,

- zákon č. 413/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi,

- zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů spolu s nařízením vlády č. 495/2004, kterým se provádí zákon č. 227/2000, a vyhláškou Úřadu pro ochranu osobních údajů č. 378/2006 o postupech kvalifikovaných poskytovatelů certifikačních služeb.

Dále zde můžeme zařadit normy, kterou jsou pro zavádění systému bezpečnosti takovými bezpečnostními standardy:

- ISO/IEC 17799:2005, která vychází z mezinárodní normy ISO/IEC 17799:2000 a obsahuje postupy pro řízení bezpečnosti v 11 částech a 39 oblastech bezpečnosti. Jde o všeobecně uznávaný soubor doporučení, součásti popisu jednotlivých opatření je také popis způsobu implementace. V roce 2006 vyšla v ČR jako norma ISO/IEC 17799:2006 po změně ISO/IEC 27002:2007 (jejími částmi jsou např. pojetí a modely bezpečnosti informačních technologií, řízení a plánování bezpečnosti informačních technologií, techniky pro řízení informačních technologií, výběr ochranných opatření, ochranná opatření pro externí spojení).

- ISO/IEC 27001:2005 obsahuje požadavky na systém řízení bezpečnosti informací. Podporuje procesní způsob řízení bezpečnosti, definuje metodický rámec, ve kterém se na základě analýzy rizik vybírají opatření doporučená normou ISO/IEC 17799:2005. Požadavky v této normě jsou definovány jako povinné. Podle normy ISO/IEC 27001:2005 probíhá certifikace ISMV ve firmách a institucích. Dále zde řadíme i českou normu ČSN ISO/IEC 27001/2006.

- ČSN ISO/IEC 15408, informační technologie, bezpečnostní techniky, kritéria pro hodnocení informační technologie,

- ČSN ISO/IEC 10181, informační technologie, propojení otevřených systémů, bezpečnostní struktury otevřených systémů,

- ČSN ISO/IEC 11770, informační technologie, bezpečnostní techniky, správa klíčů.

Stěžejním zákonem je zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, který hovoří v ust. § 1 o tom, že „Tento zákon v souladu s právem Evropských společenství, mezinárodními smlouvami, kterými je Česká republika vázána a k naplnění práva každého na ochranu před neoprávněným zasahování do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.“ V ust. § 3 je stanovena působnost tohoto zákona v tomto znění:

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

odst. 2, Tento zákon se vztahuje na veškeré zpracování osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky.

odst. 3, Tento zákon se nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu.

odst. 4, Tento zákon se nevztahuje na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovány.

odst. 5, Tento zákon se dále vztahuje na zpracování osobních údajů,

jestliže se právní řád České republiky použije přednostně na základě mezinárodního práva veřejného, i když správce není usazen na území České republiky,

jestliže správce, který je usazen mimo území Evropské unie, provádí zpracování na území České republiky a nejedná se pouze o předání osobních údajů přes území Evropské unie; v tomto případě je správce povinen zmocnit postupem podle § 6 na území České republiky zpracovatele.

Jestliže zpracování provádí správce prostřednictvím svých organizačních jednotek umístěných na území Evropské unie, musí zajistit, že tyto organizační jednotky budou zpracovávat osobní údaje v souladu s národním právem příslušného členského státu Evropské unie.“

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů vznikl na základě zákonu č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, který byl účinný od 1.6. 1992 a byl zrušen ke dni 1.6. 2000.

V současné době platná legislativa ukládá provozovatelům informačních systémů, kteří provádějí správu dat, aby tyto data náležitě chránili proti neoprávněnému zneužití. Ochrana osobních údajů je jedna z nejdůležitějších oblastí v rámci vývoje nových informačních technologií. S velkým rozvojem elektronizace a informatiky bude ochrana zpracovávaných dat stále aktuálním problémem. Vláda České republiky ve svém dokumentu „Strategie rozvoje služeb pro informační společnost“ s označením „Vize ČR jako jedna z pěti nejlepších zemí EU v úrovni rozvoje e-Governmentu“ uvádí, že „Strategie bude implementována prostřednictvím řady vzájemně provázaných projektů; tyto projekty jsou rozděleny do pěti programových oblastí. Základním cílem strategie je transformovat a zjednodušit procesy používané dnes ve Veřejné správě tak, aby využívaly moderních komunikačních a informačních technologií způsobem obdobným jejich využívání ve sféře komerční. Moderní komunikační a informační technologie totiž umožňují vytvořit zcela nové portfolio služeb veřejné správy, zjednodušující zásadním způsobem komunikaci občanů i firem s veřejnou správou i mezi subjekty veřejné správy navzájem. Současně lze výrazně zvýšit efektivitu výkonu veřejné správy bezpečným sdílením nejčastěji používaných informací v jednotlivých agendách.

Prioritními oblastmi jsou:

- základní registry a identifikace, registr územní identifikace a nemovitostí; registr obyvatel; registr osob; registr práv a povinností,
- univerzální kontaktní místo, asistovaná i samoobslužná komunikace s veřejnou správou, portál veřejné správy a jednotlivé agendové portály, systém datových schránek,
- zaručená a bezpečná elektronická komunikace, v rámci úřadů a také mezi úřadem a občanem s dodržování bezpečnostní politiky,
- digitalizace datových fondů a jejich archivace,
- vlastní služby pro informační společnost:

a) zdravotnictví, důchodová péče, školství,

b) veřejná správa v užším smyslu, soudní, správní a daňová řízení, vedení elektronických spisů,

c) správa aktiv státu a samospráv, zejména evidence majetku, rozpočtování, státní pokladna, nakládání s majetkem a penězi, veřejné zakázky, dotace.

4 Analýza současného využití moderních informačních technologií v rámci instituce Městského ředitelství Policii České republiky

4.1 Policie ČR, popis a schéma

Jako každá jiná instituce působící v rámci veřejné správy, tak i Policie České republiky využívá moderních informačních technologií a jejich používání je pro práci této instituce nezbytné. Policie ČR je součást veřejné správy a řadí se k orgánům, které přímo vykonávají státní moc. Pro institucionálních chod této součásti jsou nezbytné moderní aplikace informačních technologií. Nutností je včasné a přesné předávaní informací. Policie ČR je celostátní instituce, která je tvořena organizačními články od nejnižších organizačních článků po nejvyšší, které jsou dále rozděleny podle působnosti. Obecně se policie dělí na vnější službu a vnitřní službu. Vnější služba jsou organizační články vykonávající službu v rámci pořádkové policie a vnitřní služba jsou organizační články vykonávající službu v rámci kriminální policie. Toto dělení lze také specifikovat na uniformovanou policii a policii službu vykonávající v civilním oděvu. Organizační schéma celorepublikového složení policejních složek je uvedeno v příloze. Informační systém Policie ČR je založen na principu intranetu, tedy vnitřní institucionální sítí. Tento systém je velmi výhodný v tom, že data sdílená v tomto systému nejsou tak zranitelná, jako data kolující na masově přístupné sítí. Interní síť policie propojuje všechny organizační články tak, aby informace v rámci těchto článků mohly být rychle, přesně a spolehlivě předávány. Jednotlivé útvary Policie ČR jsou strukturálně členěny od policejního prezidia, které zastřešuje všechny útvary, směrem k nižším organizačním článkům. Od policejního prezidia následují jednotlivá krajská ředitelství Policie ČR a poté následují jednotlivé Okresní ředitelství a Městská ředitelství. Městská ředitelství jsou dále členěny na jednotlivé oddělení. V resortu Policie ČR jsou i oddělení, které mají celostátní působnost a ne v rámci určitých teritorií, jak je tomu u Krajských a Městských ředitelství. Organizační články Policie ČR mají přesně vymezené úkoly a působnost. Tyto úkoly a působnost upravuje zákon č.273/2008 Sb., o Policii České republiky, kde je vše taxativně zakotveno. Policie ČR je jednotný ozbrojený bezpečnostní sbor, který slouží veřejnosti. Jejím úkolem je chránit bezpečnost osob a majetek a veřejný

pořádek, předcházet trestné činnosti, plnit úkoly podle trestního řádu a další úkoly na úseku vnitřního pořádku a bezpečnosti svěřené jí zákony, přímo použitelnými předpisy Evropských společenství nebo mezinárodními smlouvami, které jsou součásti právního řádu. Policie působí na území České republiky, nestanoví-li zákon nebo jiný právní předpis jinak. Policie ČR jako instituce veřejné správy provádějící výkon státní moci, využívá veškerých zákonných a dostupných prostředků potřebných pro tento výkon. Počty příslušníků Policie ČR, vybavení a rozmístění je přesně dané a upravené zákonem. Policie ČR, jako každá jiná instituce veřejné správy při výkonu své působnosti je nucena využívat informačních zdrojů a následně pracovat s těmito informacemi. Tyto získané informace jsou poté analyzovány a podle potřebnosti využívány. Jelikož instituce veřejné správy se blíží k občanovi a jsou mu nápomocny tak, i Policie ČR v současné době změnila svou tvář z ryze represivní složky na složku, které je připravena pomáhat a chránit občana. O tomto hovoří i nápis v reflexních pruzích služebních vozidel. Obsah tohoto nápisu znamená, že i policejní složka jako taková musí v současné době jít blíže k občanovi a ukázat mu, nejen represivní tvář, ale naopak pomoci mu v obtížných životních situacích. Také to znamená, že se musí přizpůsobit občanům a jejich potřebám, tedy přizpůsobit se moderním skutečnostem v rámci informatiky a elektronizace veřejné správy. Policie ČR si už nevystačí s technikou, která byla osvědčená léty, ale potřebuje nové, moderní, pružné technologie, aby mohla předcházet kriminalitě a účinně bojovat proti trestné činnosti. Základním nástrojem proti tomuto sociálně patologickému jevu, jakým kriminalita bezesporu je, jsou informace. Tyto informace je třeba rychle získat, analyzovat a využít potřebným způsobem. Už jsou pryč ty doby, kdy se archív vedl v písemné podobě a jednotlivé informace se musely pracně vyhledávat. Současné technologie nám usnadnily život a potřebné informace se dají vyhledat prakticky všude. V rámci Policie ČR to znamená, že potřebné informace pro svou práci si policie shromažďuje a vyhodnocuje samostatně a k tomuto účelu si vede různé technologické aplikace k uskladnění a vyhodnocování těchto informací.

4.2 Popis moderních informačních technologií v rámci oddělení MŘ PČR

Každé jednotlivé oddělení a pracoviště Policie ČR se vybavuje podle jeho konkrétních úkolů a působnosti. V této části se budu zabývat praktickou situací ve vybavenosti jednotlivého oddělení v rámci Policie ČR. Jedná se o oddělení Služby kriminální policie a vyšetřování v rámci Městského ředitelství Ostrava. Toto oddělení má v současné době 23 pracovníků. V přímém výkonu služby je 19 pracovníků a 4 pracovníci jsou administrativního charakteru. Oddělení SKPV pokrývá činnost operativní a vyšetřovací. Operativní činnost je činnost zaměřená především na terénní práci a proto členění těchto zaměstnanců je ve dvojicích po dvou. Vyšetřovací činnost je charakterově převážně kancelářskou prací. Vyšetřovací činnost provádí v podmínkách tohoto oddělení 8 pracovníků. Toto oddělení má své prostory k pracovní činnosti, v kancelářích je převážně umístěno po dvou pracovnicích. Oddělení je vybaveno telefonními linkami ve všech kancelářských prostorách, prakticky na každého zaměstnance je přiděleno telefonní číslo. Centrálně je umístěn faxový přístroj, kopírka, 2 x scanner a tři síťové tiskárny. V rámci tohoto oddělení je umístěno 22 počítačových sestav, kdy ne všechny jsou stejných parametrů a určeny ke stejnému použití. Všechny počítačové sestavy jsou připojeny na vnitřní policejní síť intranet a mohou využívat dostupné aplikace z tohoto systému. Pouze jedna počítačová sestava je umístěna samostatně, mimo vnitřní síť a je připojena k veřejnému internetu. Tato počítačová sestava je izolovaně připojena samostatně k internetu a to hlavně z bezpečnostních důvodů. Počítač je k využití ve společných prostorách oddělení a plní funkci jen k možnému připojení k internetu z důvodu využití nějakých potřebných informací, které nejsou dostupné na interních počítačích. Ostatní počítače tvoří síťovou jednotku, umožňující využívat síťových tiskáren a aplikací. V současné době, v rámci resortu Policie ČR běží program ETŘ (Elektronické trestní řízení), který v rámci tohoto oddělení běží od roku 2008 a je stěžejním systémem pro chod tohoto oddělení.

4.2.1 Elektronické trestní řízení

Je to informační systém vytvořen na bázi webové aplikace spustitelné v prohlížeči Internet Explorer. V rámci Městského ředitelství Policie ČR v Ostravě byl tento systém zaveden do praxe začátkem roku 2008. Tento systém je utvořen pro potřeby Policie ČR, státních zastupitelství a soudu. Hlavním produktem tohoto

systému je vytvoření elektronického spisu, který je v současné chvíli přístupný více oprávněným uživatelům. Z důvodu, že Policii ČR pracuje s citlivými daty a především s údaji o osobách, které jsou chráněny zákonem, tak musí tato aplikace splňovat bezpečnostní parametry, aby k únikům těchto dat nedocházelo a nemohlo dojít. Elektronický spis je systém, který umožňuje vést spis v elektronické podobě a v případě potřeby do něj v jaké-koliv fázi nahlížet a provádět operace. Tato aplikace přináší větší přesnost, rychlost a kontrolovatelnost při vypracování tohoto spisového materiálu. Elektronický spis zatím není celorepubliková záležitost, ale je veden v rámci jednotlivých Krajských ředitelství Policie ČR. Je propojen s různými databázemi, podle potřeb využití. Pro potřeby čerpání dat k fyzickým a právnickým osobám, tak je systém propojen s celostátní evidenci fyzických a právnických osob, s Rejstříkem trestu a s dalšími interními systémy v rámci Policie ČR. Elektronické trestní řízení je v současné době hlavním pracovním nástrojem policistů. Při jakém-koliv podnětu, oznámení nebo při řešení problémů, sepíše službu konající policista na místně příslušném organizačním článku záznam o této situaci. Podle vyhodnocení této situace ji zadá do systému ETŘ. Tento systém rozlišuje tři roviny zápisu.

Rozdělení zápisu podle obsahu:

- číslo jednací, je každá událost, která nemá znaky trestného činu a nejedná se o přestupek, jde převážně o blokovou pokutu, vyřízení žádosti, interní vyřizování apod.,
- trestný čin, jednoznačně charakterizováno v trestním zákoníku,
- přestupek, jednoznačně charakterizováno v přestupkovém zákoně.

Po vyhodnocení zápisu se tento dle obsahu zavede do systému ETŘ a označí jako číslo jednací, trestný čin nebo přestupek a systém pro tento zápis vygeneruje číslo jednací. V systému ETŘ jsou tedy ve stejném roce pod jedním číslem zavedeny tři odlišené události, které jsou rozlišeny jen zkratkou uvedenou v číslu jednacím. Číslo jednací se skládá ze znaků písmen, čísel a znamének.

Například KRPT-1234-3/TČ-2010-070700-008 po rozdělení jednotlivých označení znamená:

- KRPT, znamená označení příslušného krajského ředitelství Policie ČR, kde je spis veden,

- 1234, je to označení čísla spisu, pořadové číslo spisového záznamu od začátku roku,

- 3, pořadové číslo označení vzniku dokumentu v rámci konkrétního trestního spisu,

- TČ, označení, že jde o trestný čin, PŘ přestupek, ČJ číslo jednací,

- 2010, rok vzniku trestního spisu,

- 070700, kódové označení konkrétního útvaru v rámci Policie ČR, který elektronický spis zpracovává,

- 008, kódové označení konkrétního zpracovatele, který elektronický spis zpracovává v rámci konkrétního oddělení (položka není povinná).

Po provedení generace č.j., po zadání vstupních dat a uložením těchto dat, je spis zanesen do systému. Tento spis je členěn formou záložek, kdy na úvod se vyplní popis deliktu, právní označení a kvalifikace, způsob provedení, způsobená škoda, datum spáchání, útvar, který věc přijal, útvar, který věc šetří. Z této záložky se pokračuje dále a vyplní se místo spáchání skutku, popíšou se podrobně údaje k lokalizaci včetně možnosti zanést GPS souřadnice. Dále se pokračuje k osobám, které jsou účastny ve spisu. K těmto se vypíši údaje směřující k totožnosti těchto osob a údaje k právnímu postavení této osoby ve věci. Právní postavení je důležité pro následnou práci v systému, jelikož každá osoba má jiná práva a postavení. Po zadání základních údajů k osobě se poté tyto údaje ztotožní v rámci registru obyvatel a tímto dostaneme ke spisu data, která jsou přesná podle centrální evidence obyvatel a takto přesná data se přenesou do systému ETŘ. Pak se doplní k osobě další upřesňující a potřebná data, doplní se současné bydliště, doručovací adresa a zaměstnavatel a kontakty na osobu. Takto zapsané základní údaje se uloží do systému a pak dle potřeby jde zapsat další potřebné údaje pro práci Policie ČR. Jedná se o údaje k odcizeným věcem, zadrženým osobám, zajištěným stopám a další. Následně po provedení základního vkladu dat do tohoto systému, tak jednotliví pracovníci můžou zakládat v systému dokumenty, které jsou už

připravené v určitých aplikacích. Jedná se o protokol o trestním oznámení, protokol o zadržení podezřelého, protokol o zadržení obviněného a o mnoho dalších protokolů potřebných v rámci trestního řízení. Protokoly jsou v nabídce strukturálně řazeny. Tyto a jiné protokoly jsou koncipovány tak, že určité údaje jsou automaticky vyplňovány a další jsou nabízeny k doplnění. Vyplňování údajů k osobám je v těchto protokolech velmi přesné, neboť se už čerpá z údajů, které byly do systému vloženy prostřednictvím centrální evidence obyvatel a jsou tedy přesné a nijak nezkreslené. Tato protokolace velmi šetří čas a zvyšuje tím kvalitu a kvantitu práce policistů. Protokoly jsou vytvořeny tak, aby jejich uspořádání v nabídce bylo logicky uspořádané podle kategorií a potřebnosti. Tento systém elektronického spisu není limitován počtem pracovníků, kteří pracují s tímto systémem. Je možné, aby pracovalo více pracovníků v rámci jednotlivého spisu. Jeden může provádět protokolaci s poškozeným subjektem, druhý si může psát záznam o provedených opatřeních k věci a další může upravovat vstupní data, popřípadě další můžou pracovat na dalších dokumentech v rámci systému. Tento systém také umožňuje, že protokolaci v písemné podobě můžou sledovat další osoby, které nejsou přímo účastny v místnosti, kde zrovna protokolace probíhá, což je nespornou výhodnou ve složitých a komplikovaných trestních případech. Policista sleduje zápis a může vyhodnocovat fakta na které lze poté reagovat, tento policista vůbec nemusí být přítomen v rámci budovy, ale stačí mu k tomu jen služební počítač Policie ČR a přístupové heslo k této aplikaci a k tomuto konkrétnímu spisového materiálu. Po provedeném zápisu dat do aplikace jsou tato data kontrolována administrativním pracovníkem v rámci oddělení a poté vedoucím služebním funkcionářem jsou zadány pokyny ke splnění. Tyto pokyny slouží k doplnění spisového materiálu o potřebné skutečnosti, aby byl spisový materiál při svém ukončení kompletní a mohlo být rozhodnuto na základě relevantních skutečností. Vedoucí služební funkcionář taktéž zadá v systému pracovníka nebo pracovníky, kteří spis budou zpracovávat se stanovením konkrétního data k přístupu k tomuto spisu. Takto přidělený spisový materiál si konkrétní pracovník převezme a zároveň potvrdí převzetí pokynu od služebně nadřízeného funkcionáře. Následně si vypracuje vlastní plán vyšetřování, ve kterém si zadá konkrétní úkoly, které bude plnit s daty splnění. Tyto data poté systém hlídá a upozorňuje pracovníka zpracovávající spis na splnění těchto úkolů. Spis je veden komplexně v elektronické podobě a paralelně vede oddělení spis také papírový v písemné podobě. V současné době je stále na prvním

místě spis veden v písemné podobě a elektronicky spis je součást toho písemného spisu. Písemný spis se také archivuje v archívech po dobu skartační doby, která je u různých věcí rozdílná. K elektronickému spisu je možné připojovat v neomezené míře datové soubory a to v různé podobě. Policista tedy primárně pracuje v elektronickém trestním řízení, kde zpracovává případy, pokud je tento případ nutný k zavedení do dalších aplikací v rámci Policie ČR, lze toto provést a převést potřebná data do jiných aplikací, kde se potom uloží. Je tedy nezbytné, aby data v elektronickém trestním řízení, potažmo v trestním spise byla objektivní, skutečná a aktualizována. Je nezbytné, aby spis písemný byl totožný jako spis elektronický. Samozřejmostí při práci s popisovaným systémem je bezpečnost zpracovávaných dat. Tato bezpečnost je zajištěna tím, že do elektronického spisu nemůže nahlížet každý, kdo má přístup do informačního systému Policie ČR. Nahlížet do elektronického spisu je možné jen na základě zadání přiděleného hesla pro informační systémy Policie ČR a také musí být ten uživatel, který chce do spisu podrobněji nahlédnout zpřístupněn do spisu oprávněnou osobou na určitém funkčním zařazení. Zároveň když dojde k nahlédnutí do určitého spisu je o tom elektronický záznam. Systém je navržen a uzpůsoben tak, aby mohl být využíván nezávisle na kterém-koliv organizačním článku Policie ČR, aby přispěl k větší kontrole policejní práce, rychlosti a pružnosti. Je nutné se zmínit, že se zde jedná i jakýsi antikorupční prostředek, jelikož blokové pokuty, které policista vydá, jsou neprodleně zavedeny do systému pod č.j. a nemůže poté dojít k ovlivňování nebo nějakému vyřizování těchto pokut. Prakticky každá řešená situace a oznámena věc v rámci resortu Policie ČR je zaevidována a transparentně řešena. Elektronický spis není určen jen pro Policii ČR, ale má také sloužit pro potřeby státního zastupitelství a soudu. Státní zastupitelství je nezbytnou součásti trestního řízení. Výkon nad zákonnosti trestního řízení vykonává státní zástupce což je upraveno v trestním řádu. Státní zástupce a policejní orgán jsou dvě složky, které spolu v rámci trestního řízení úzce spolupracují. Z tohoto důvodu je zřejmé, že elektronický spis byl zaveden nejen pro policejní složky pro které primárně pracuje v současné době, ale také pro státní zastupitelství. Státní zástupce mnohdy potřebuje adekvátně rozhodovat ve věcech a být přímo zainteresován na vyšetřovacích úkonech. Je tedy nezbytné, aby měl rychlý přístup k informacím v té konkrétní kauze, což mu zaručuje elektronicky trestní spis. Státní zástupce při přístupu do tohoto spisu mohl provést obeznámení s určitou věcí a poté dát příslušné pokyny k doplnění

a kontrolovat si plnění těchto pokynů, aniž by musel osobně věc konzultovat, nebo si vyžadovat trestní spis vyhotovený v papírové podobě. Současná praxe je taková, že Okresní státní zastupitelství v Ostravě není připojeno k elektronickému trestnímu řízení, jako uživatel systému. Spisy jsou na státní zastupitelství doručovány stále osobně v papírové podobě. Tento krok bude do budoucna určité nutný, ale v současné situaci a fázi elektronického trestního řízení není realizovatelný. Jak z důvodu technických, tak bezpečnostních. Elektronické trestní řízení bude dále pokračovat ve své inovaci, vytvářejí se stále nové verze a nahrávají se nové potřebné dokumenty tak, aby práce s tímto systémem byla přehledná a rychlá. Systém jde cestou k celostátní databázi. Tento systém lze využívat také v tipování trestné činnosti, statistickém zpracování apod., jelikož podle určitých vyhledávacích znaků si lze najít z tohoto systému určité případy. Tyto případy lze hledat podle lokalit, kde došlo ke spáchání činu. Také podle jména osob, které jsou zavedena v systému. Dále lze hledat osoby jako takové a získávat k nim potřebné informace, které následně vedou k zjištění současného pobytu této osoby. Přes uvedený systém je také možné zadávat úkoly i různým jiným útvarům Policie ČR, kterým se tyto úkoly zobrazí. Tyto útvary si úkoly musí převzít a následně splnit. Odpadá tedy zdlouhavé doručování těchto úkolů běžnou poštou. Elektronické trestní řízení je taktéž propojeno s centrálním registrem fyzických a právnických osob, ze kterých čerpá potřebná data. Také je propojen s Rejstříkem trestu, čímž odpadá pracné a zdlouhavé vyřízení tohoto rejstříku v minulosti. Také se ETŘ propojilo se systémem datových schránek, jelikož také Policie ČR jako která-koliv jiná instituce veřejné správy je povinna tohoto informačního systému využívat a primárně komunikovat v rámci datových schránek. Elektronické trestní řízení je ryze systémem k evidencí událostí v rámci Policie ČR, který zpřehledňuje práci Policie ČR, dává nové možnosti při zpracování věcí. Vnáší do práce Policie ČR flexibilitu a transparentnost a nabízí prozatím jediný komplexní systém v rámci resortu. V rámci popisované instituce je tento systém ve stádiu ostrého provozu od roku 2008 a od začátku roku 2010 se do tohoto systému plně implementoval Informační systém datových schránek. Přímo z jednotlivých trestních spisů lze zasílat žádosti a různé potřebné formuláře prostřednictvím datových schránek k dotčeným institucím veřejné správy a jiným právnickým osobám.

4.2.2 Kriminalisticky sledovaná událost

Jedná se o celostátní informační systém sloužící pro potřeby Policie ČR při výkonu státní moci. Cílem tohoto systému je zjednodušit, zrychlit a zefektivnit získávání
a využívání informací, které napomáhají policistům při odhalování a vyšetřování trestné činnosti, případně jejímu předcházení. Systém KSU zavedl nové technologické prvky pro analytické činnosti s kriminalistickými daty, jejichž cílem je mimo jiné zajistit jednotný datový tok do centra, dostupnost a využitelnost informací pro všechny oprávněné uživatele. Současně zajišťuje uživatelskou přijatelnost v moderním technologickém prostředí. Provozování tohoto systému je zajišťováno na intranetu Policie ČR. Primárně tento informační systém není určen pro zpracovávání oficiálních statistik kriminality, ze kterých by bylo možno čerpat údaje o celkové kriminalitě, objasněnosti apod. K tomuto účelu jsou určeny jiné provozované informační systémy v rámci resortu Policie ČR. Do systému KSU patří jen údaje potřebné z hlediska operativně-taktického rozhodování. Systém KSU je koncipován jako centrální evidence a proto jsou zde upravena jednotná pravidla vkládání dat do tohoto systému tak, aby tyto data mohly být dle potřebnosti využitelná. Data, která jsou vkládaná do tohoto systému musí být relevantní a validní. Systém provádí evidenci vybraných trestných činů a odcizených věcí, kdy nám poté nabízí zpětné hledání v tomto systému k nalezení konkrétních trestných činů podle různých kriterií. Také lze vyhledávat osoby pachatele a trestné činy těmito osobami spáchané a lze vyhledávat i odcizené věci. Tyto skutečnosti lze vyhledat podle různých kriterií, které se zadávají do systému. Systém KSU představuje seznam trestných činů a s tím spojených náležitostí. V systému se chronologicky eviduje trestný čin nebo určený skutek. K tomuto se zaznamenávají veškeré poznávací znaky.

Mezi tyto patří:

- doba a místo spáchání skutku,
- výše způsobené škody,
- právní kvalifikace dle zákona,

- stručný popis skutku,
- znaky skutkového jednání,
- příslušnost útvaru, který věc přijal a šetří,
- seznam a popis odcizených věcí včetně identifikačních znaků,
- seznam a identifikační údaje zúčastněných osob na konkrétním případu.

Tyto údaje nám zařazují určité skutkové jednání do struktury činů vedených v systému KSU a poté analytickou činností lze pracovat s takto získanými údaji. Vklad těchto údajů se provádí na základních článcích Policie ČR, tedy na místně příslušných Obvodních odděleních a Místních oddělení. Po provedení základního vkladu určitého skutkového jednání, které splňuje znaky zařazení do systému KSU se následně provede verifikace těchto údajů. Tato verifikace se provádí na specializovaném pracovišti a srovnávají se údaje získané z centrálních evidencí, zda tyto údaje jsou totožné v systému se skutečností. Systém KSU je v současné době jediným komplexním systémem, který eviduje celostátně trestné činy a umožňuje zpětnou analýzu těchto činů. Systém byl zaveden v roce 2003, kdy jeho využívání stanovuje příslušný Závazný pokyn policejního prezidenta č.120/2003 Sb. Pro vkládání dat do systému KSU je stanoveno, že se do něj vkládají data všech trestných činů a přestupků, kde je zjištěno výrobní číslo odcizené věci. V současné době podle platného znění trestního zákoníku se trestné činy dělí na přečiny a zločiny. Systém KSU jako takový je už technologicky překonán systémem ETŘ, ale z důvodu, že nový systém ETŘ není ještě celostátní a provozuje se v rámci krajské působnosti, tak stále se pro potřeby Policie ČR využívá systém KSU. Tento je propojen se systémem ETŘ v oblasti čerpání dat z tohoto systému. Primárně se vkládají data do systému ETŘ a následně pokud je potřeba tak se tyto data překlápějí do systému KSU.

4.2.3 eSIAŘ

Už ze samotného názvu vyplývá, že se jedná o elektronický celostátní systém policejních složek, vedený v rámci intranetu, který je založen na principu centrální

evidence všech policistů ČR, všech organizačních článků a všech potřebných dokumentů a inovací se kterými musí být policista prokazatelně seznámen. SIAŘ je sbírka interních aktů řízení. Malé e znamená značku pro elektronickou podobu. Vznik a používání tohoto systému v rámci Městského ředitelství Policie ČR v Ostravě je datován na konec roku 2008. Tento systém eviduje všechny policisty ČR s jejich aktuálními údaji a služebním zařazením. Také eviduje veškeré písemnosti potřebné pro chod Policie ČR. Jeho cílem je, aby každý policista při svém nástupu do zaměstnání, provedl přihlášení do tohoto systému a seznámil se všemi aktuálním písemnosti, které jsou pro něj určené. Tyto písemnosti si přečetl, podle potřeby vytisknul a následně označil prohlášení, že se s tímto řádně seznámil. Do tohoto systému jsou zařazované písemnosti centrálně a poté vedoucí jednotlivých organizačních struktur označí písemnosti se kterými musí být nebo můžou být seznámení jejich podřízení. Tyto písemnosti se poté objeví v elektronické podobě v seznamu dokumentů jednotlivých policistů. Tímto způsobem seznamování se novými právními předpisy a postupy v rámci Policie ČR, odpadá zdlouhavé osobní školení na kterém si každý policista musel dělat výpisky nebo si pořizoval kopie potřebných dokumentů, aby se s nimi mohl později seznámit. Dochází zde k úspoře času a materiálních hodnot. Tímto se také zlepšuje informovanost jednotlivých pracovníků. Odpadají zde také nejasnosti o seznámí či neseznámení s daným materiálem, a je snadno dohledatelná skutečnost, kdo a kdy se s předmětným materiálem seznámil. Přihlašování do tohoto systému se provádí na základě zadání kombinace přístupového kódů jednotlivého policisty a jeho osobního hesla, které musí mít určitý počet specifických znaků, aby bylo přijato do systému. Znamená to, že heslo musí obsahovat určitý počet znaků v kombinaci s velkými, malými písmeny a číslicemi. Zjednodušeně lze hovořit o tomto systému, že se jedná o evidenční a doručovací systém potřebných dokumentů se seznamem všech adresátů. Služební vedoucí funkcionář, na své úrovni vydá rozhodnutí nebo jinou písemnost a tuto doručí všem komu má být určena, tito ji poté vloží do schránek jednotlivých policistů, kteří se s touto písemnosti seznámí. To vše se děje v reálném čase podle elektronických a technologických dispozic systému. Tento systém byl aplikován v rámci resortu policie v průběhu roku 2006. Ve vztahu k tomuto systému se nejedná o systém evidence trestných činů, přestupků či jiných událostí v rámci policejní agendy, ale je to systém k evidenci organizačních struktur, policistů

a vydaných dokumentů určených k seznámení příslušníkům Policie ČR, podle jejich dispozic.

4.2.4 Centrální evidence obyvatel

Pro potřeby působnosti Policie ČR je nezbytné, aby měla přístup k informacím o osobách. Z důvodu těchto potřeb využívá Policie ČR systém centrální evidence osob s interním názvem „Berunka“. Tento systém je čistě evidencí a shromažďuje data o osobách pro potřeby policejní činnosti. Jedná se o sdružený systém, který v sobě aplikuje více jiných systémů tak, aby byl komplexní přístup k potřebným datům. Sytém Berunka je určen k vyhledávání potřebných údajů podle zadaných kriterií, hlavně se jedná o hledání určitých osob a údajů k těmto osobám. Základem tohoto systému jsou data z celostátního centrálního registru osob a poté data získaná při činnosti policejních složek v rámci své působnosti.

Seznam kriterií pro vyhledávání:

- podle základních údajů k osobě, jméno příjmení a datum narození,
- podle zadání intervalu data narození od do s uvedením jména a příjmení,
- podle zadání místa trvalého bydliště osoby.

Toto jsou tři základní možné vklady vstupních údajů dat do evidence k vyhledání konkrétní osoby. Po provedení specifikace konkrétní osoby je možné u této osoby nechat vyhledat potřebné údaje podle potřebnosti.

Seznam údajů, které evidence nabízí vyhledat k určité osobě:

- vlastnictví motorového vozidla,
- údaje o možném pátrání po osobě,
- údaj o možném trestním stíhání osoby v rámci policejního orgánu,
- vlastnictví zbraně a zbrojního průkazu,
- zákaz pobytu osoby v určité lokalitě,
- vlastnictví řidičského oprávnění s uvedením konkrétních údajů,

- údaje z evidence cizinců.

Tyto a další údaje lze z evidence čerpat. Jelikož se jedná o údaje ke konkrétním osobám, které podléhají zákonu o ochraně osobních údajů, nemůžou být tyto informace k dispozici každému, ale jsou přístupné jen na základě určitého zmocnění a příslušného přístupového kódu. Pokud dochází k čerpání údajů z této evidence, tak musí být vždy uveden relevantní důvod k čerpání těchto údajů s uvedením spisové značky případu pro který jsou údaje čerpány. Evidence také eviduje vstupy k vyhledávaným osobám a zpětně lze dohledat, kdy a jaké konkrétní informace byly z evidence čerpány. Evidence je také technologicky vybavena tak, že pokud dojde k delší nečinnosti v tomto systému, tak dojde k automatickému odpojení evidence a nové připojení je opět po zadání přístupového kódu. Systém berunka je také propojen se systémem ETŘ, kdy na základě tohoto propojení, systém ETŘ čerpá přesná data k osobám. Tyto se poté nezkreslené zavádějí do systému ETŘ a následně se s těmito daty pracuje. Data jsou čerpána pro systém ETŘ z evidence obyvatel systému Berunka a ne opačně. Tímto je zaručeno, že data, které se takto získají jsou přesná a ničím nezkreslená. Tímto je zaručena jejich validita. I toto čerpání dat v rámci těchto systémů není automatické, ale je podmíněno zadáním přístupového kódu, na základě, kterého jsou tyto údaje dostupné. I tyto vstupy a čerpání dat jsou zaznamenány pro pozdější využití.

Dále policejní složky pro svůj chod využívají různé další centrální evidence tak, aby měly co nelepší a nerychlejší přístup k potřebným informacím. Policie ČR pracuje s různými informacemi podle potřebnosti a nejedná se o práci jen s určitým druhem informací. Pro tyto účely využívá různé další evidence, jako jsou evidence znalců, tlumočníků a advokátu. Také evidence odcizených uměleckých děl, věcí a také používá spoustu jiných evidencí a seznamů vedených v různých aplikacích, které jsou zpřístupněny přímo nebo také po zadání příslušného přístupového kódu.

4.2.5 Událost

Toto je systém, který pracuje na základě předávání informací, které jsou chronologicky řazeny v elektronickém hlášení. Jedná se o seznam skutků, které se staly v rámci Policie ČR za určité období v určité oblasti, stručně řečeno jde o zápis

všech událostí, které se staly za určitou časovou jednotku v určité specifické oblasti spadající do místní příslušnosti jednotlivé policejní složky, nebo-li útvaru Policie ČR. Jde o aplikaci do které se zapisují veškeré potřebné skutečnosti k určitým případům a tyto informace se poté elektronicky posílají pracovníkovi, který je zpracovává dále podle důležitosti a posílá dalším subjektům k seznámení. Data získaná v tomto systému se adresně nerozesílají konkrétním pracovníkům osobně, ale každý kdo má potřebné oprávnění, může do systému vstoupit na základě přístupového kódu a čerpat informace. Jde o to, aby policista měl přehled o situaci, která se v jeho služebním obvodu stala za období ve kterém nebyl přítomen a podle potřebnosti se s touto situací seznámil. Jde o základní data a pro upřesnění věci je nutné čerpat další data ze systému ETŘ. Data do systému Událost se také čerpají ze systému ETŘ a niko-li obráceně. S postupnou realizací celostátního ETŘ, je pravděpodobné, že systém Událost zanikne a pozbude své potřebnosti. Skutková událost je řazena v systému chronologicky podle toho, kdy se stala a kde a o jaký stupeň důležitosti informace se jedná. Další řazení skutkových událostí je podle času jejich přijetí příslušným policejním orgánem a také podle toho, který konkrétní policejní orgán zařazenou věc do systému prověřuje.

Hlavní dělení v systému Událost je podle:

- celostátního hlášení,
- krajského,
- okresního.

Toto dělení se vztahuje ke struktuře organizačních článků v rámci Policie ČR, které mají ke zveřejňovaným informacím přístup. Z taktických důvodů a ochrany osobních údajů, lze určitý druh svodných událostí označit jako nezveřejňované, čímž se zamezí zobrazování události ostatním uživatelům. Toto je zejména důležité, jelikož tento systém je ve velké míře využíván speciální službou v rámci Policie ČR, která předává informace do sdělovacích prostředků ke zveřejnění.

4.3 Současné moderní trendy informačních technologií aplikované v rámci instituce MŘ PČR

Dnešní trendy v informačních technologiích v rámci oddělení MŘ PČR jsou, aby byly informační a pracovní systémy Policie ČR kompatibilní a sjednocené a nemuselo se provozovat více různých druhů systémů. Cesta směřuje k vytvoření komplexního systému, který by v sobě zahrnoval veškeré potřebné informace a pracovní prostředky. Současná situace je taková, že ještě se provozují systémy, které jsou stále potřeba, ale jejich účel už je překonán systémem ETŘ, který je zaváděn do celostátní praxe. ETŘ je v současné době primárním a komplexním systémem pro potřeby Policie ČR, který plně vyhovuje současným nárokům na informatiku veřejné správy. Informatika v rámci institucí veřejné správy a také konkrétního oddělení o kterém hovoříme, už má své pevné místo a je ji možno jen vylepšovat hardwarovým a softwarovým vybavením. Směr informatiky je takový, aby odbourala přebytečnou byrokracii, která stále ještě existuje. Je třeba řádně využívat dostupných informací. V rámci popisované instituce se v současné době, trendy projevují tak, že počítačový systém je důležitou součásti práce a na každého pracovníka připadá prakticky jedna počítačová jednotka. Bez počítačové sestavy by pracovník nemohl odvádět svou práci a neměl by přístup k potřebným datům. Praxe je taková, že při příchodu do práce se pracovník musí přihlásit kódovaným heslem na svém počítači a musí provést přihlášení do systému eSIAŘ k seznámení s aktuálními dokumenty. Poté se pod svým heslem přihlásí do systému ETŘ ve kterém zpracovává přidělenou spisovou agendu. Bez tohoto systému by nemohl vůbec pracovat. Z toho plyne situace, že současná doba je až příliš závislá na elektronizaci a informatice, bez těchto prostředků by nemohla ani existovat. Počítače a připojení na vnitřní pracovní síť je nezbytnou součásti pro řádný chod instituce.

4.4 Cíl rozvoje informačních technologií v instituci MŘ PČR

Cíle jsou takové, aby vybavenost počítačovými systémy byla na velmi dobré úrovni, aby mohly být řádně využívány veškeré dostupné aplikace, neboť zastaralost počítačového vybavení je velkým nedostatkem této instituce veřejného sektoru.

Informatika a informační systémy se stále vyvíjejí a jedním z hlavním cílů rozvoje informačních technologií v rámci oddělení MŘ PČR je, aby byla lepší vybavenost informační technikou. Stěžejním cílem v rámci rozvoje je, aby systém ETŘ se podařilo implementovat v rámci celé České republiky a propojit v jeden celostátní systém, což by mělo nesporné výhody. V další řadě je zapotřebí tento systém aplikovat i v rámci státních zastupitelství a soudu. Pokud se toto podaří zdárně koncipovat a uvést do provozu, bude to mít veliký přínos časový, efektivní a úsporný. Dalšími z cílů je elektronizace veřejné správy, aby úřady mezi sebou komunikovaly primárně elektronickou poštou. Tímto by docházelo k úsporám materiálů. K těmto účelům jsou v plném běhu datové schránky, které jsou určeny ke komunikaci mezi institucemi veřejné správy, právnickými a také fyzickými osobami. Primárně jsou datové schránky určeny pro instituce veřejné správy a právnické osoby. Datové schránky se podařilo zdárně implementovat do systému ETŘ a v současné době tento systém umožňuje posílat zprávy v rámci datových schránek. Zde jde o nespornou úsporu času a nákladů na provoz byrokratických prvků. Z toho všeho vyplývá, že společnost je obklopována informatikou a proto je kladen velký důraz na lidský faktor. Jedním z dalších důležitých cílů je, aby pracovník, zaměstnanec veřejné správy byl gramotný v oblasti informatiky. Také se musíme zmínit o bezpečnostním riziku, které je jednou z hlavních priorit každé instituce při práci s daty, které podléhají zákonné ochraně. Rozvoj sebou přináší větší dostupnost dat a to sebou přináší zvětšující se riziko. Cílem v této oblasti je, aby jednotlivá data byla dána k dispozici jen těm osobám, které je skutečně potřebují a zároveň, aby čerpání těchto dat bylo podmíněno vstupní heslem a čerpání dat bylo řádně evidované.

Analýzou popisované instituce jsem dospěl k závěru, že předmětná instituce jako subjekt veřejného sektoru, využívá veškeré moderní dostupné informační technologie pro svůj provoz. Moderní technologie aplikuje v rámci instituce podle potřebnosti, tímto snižuje náklady na provoz. Tyto aplikace vycházejí ze strategie veřejné správy v rámci elektronizace a informatiky. Moderní informační technologie přispívají ke snižování nákladů na provoz, zvyšují efektivitu práce, podporují flexibilitu a odbourávají byrokratizaci. Zavádění nových prvků v rámci informatiky, vylepšuje počítačovou gramotnost. Instituce tedy využívá všech dostupných technologických vymožeností v informatice a nebrání se přirozené inovaci. Využívá

moderní informační systémy a moderní počítačovou techniku, která je obnovována za zastaralou techniku, která ještě dosluhuje na určitých součástech. Také jsem zjistil, že instituce dbá na bezpečnost přenášených a využívaných dat a vede si v rámci institucionální úrovně svou bezpečnostní politiku. Dbá na zásadném dodržování přístupu k informacím jen podle potřebnosti a oprávněnosti. Každý uživatel má určitý stupeň oprávnění a kódované heslo pro přístup k využitelným informacím. Počítačová síť je chráněna od okolních vlivů svým uspořádáním v rámci intranetu (vnitřní sítě) a používají se moderní antivirové programy. Každý zaměstnanec je řádně poučen a seznámen s tím, že nesmí zasahovat do vybavení počítačové sestavy a nesmí měnit programová nastavení. Počítačové jednotky jsou v pravidelných intervalech kontrolovány a přístup k těmto jednotkám je jen pro oprávněné uživatele. Odbornější zásady do používaných systémů a jednotek má jen oprávněný administrátor.

4.5 Zhodnocení využívání informačních systémů v rámci instituce MŘ PČR a doporučení pro jejich kladný budoucí vývoj.

Při praktickém používání informačních systémů v rámci popisované instituce bylo zjištěno, že informační systémy plní svou funkci a přispívají k větší produktivitě práce. Přispívají k odbourávaní byrokratizace a také svou transparentností potlačují korupci. Dostupnost informačních systémů i na těch nejnižších stupních v rámci Policie ČR přispívá k větší kvalitě práce a účinně pomáhá při boji s kriminalitou. Při používaní systému ETŘ, který byl zaveden do provozu začátkem roku 2008 jsem zjistil, že tento velice významným způsobem přispívá ke snížení nákladů na vedení trestních spisů. Tento systém je v současné době pilířem práce Policie ČR. Jeho zavedením do praxe se odbourává součást podružné archivace spisů a odbourává se časové prodlení k seznámení se spisem. Tento systém nabízí neomezený elektronický přístup ke kompletnímu spisovému materiálu a to z jakého-koliv místa, které je připojeno na vnitřní policejní počítačovou síť. V minulosti, pokud se někdo chtěl seznámit se spisem, musel spis fyzicky vidět na místě, kde se spis nacházel. Toto sebou přinášelo časové zdržení a navyšovalo materiální prostředky. Tento systém pracuje s přenými daty a eliminuje chybná data zúčastněných osob. Pokud jsou do systému zadávána data k osobám, které jsou zúčastněné ve věci, tak tyto data se čerpají z centrální evidence osob.

Tímto se tedy čerpají data, které nejsou ničím zkreslená a jsou z prvotního zdroje. Možnou chybou při zadávání těchto dat je, že systém ETŘ nabízí vklad dat k osobám ze svého zdroje, tedy ze své evidence, pokud už osoba byla v systému zavedena. Tyto data mohou být zkreslená a nepřesná. K tomuto bych navrhnul doporučení, aby se prvotně využívala data jen z centrální evidence osob, i v případě již existujících údajů k osobám v systému. Také jsem zjistil, že je problém s kompatibilitou systému ETŘ se systémem KSU a Událost. V systému ETŘ jsou data vedena jako základní a pak se překlápějí pro potřeby využití v systému KSU a Událost. Problém je v tom, že tyto data se musí po překlopení do těchto systémů upravit a doplnit o různé potřebné skutečnosti. V současné době není možné, aby se data ze systému ETŘ jen převedla do jiných systémů a nemusely se tyto data opravovat a doplňovat. Toto přináší zbytečné časové ztráty a komplikuje práci. Prospěla by zde jednotná úprava formy nebo přednostní využití systému ETŘ i pro potřeby informačních systémů KSU a Událost. Pro policejní činnost je zapotřebí používat různé druhy předtisků a formulářů, které slouží pro jednotlivé dílčí úkony. Systém ETŘ nabízí rychlé vklady zúčastněných osob. Což znamená, že ve formuláři se nabízí tlačítko osoba a je nám nabídnuta osoba ze seznamu osob, které jsou zavedeny ve spise. Výhodou tohoto systému je, že v určitých formulářích jsou nám nabízeny jen osoby podle označení (obviněný, svědek, oznamovatel, poškozený, jiná). Nevýhodou je, že v určitých formulářích, kde by bylo možno zadat více osob najednou, nám toto systém neumožňuje a musíme vypsat nový formulář, čímž touto operací dochází ke zbytečné časové prodlevě. Dalším záporem je, že některé z nabízených formulářů nevyhovují plně praktickým požadavkům a nelze do nich vepsat potřebné věci. Toto lze připsat k zaváděcím problémům tohoto systému, které se jistě odstraní při praktickém používání. V pravidelných intervalech dochází k inovaci systému a k implementaci nových vylepšení do praktického použití. V celém kontextu je systém ETŘ komplexním řešením spisové agendy pro práci Policie ČR v návaznosti na státní zastupitelství a soud. Systém nabízí zpracovávání spisové agendy od prvotního oznámení určitého skutku, tímto zamezuje manipulaci se spisem a odbourává korupci. Každá událost v rámci policejní práce dostává své číslo jednací a je evidována a snadno dohledatelná. Systém nabízí snadnou manipulaci, přehlednost, rychlost, přesnost práce a šetří svým pojetím finanční náklady na zpracovávání spisové agendy a následné obslužnosti. Systém ETŘ při provozu v praxi nabízí odbornou konzultaci spisového materiálů různých odborníků,

kteří mohou pocházet z různých míst. Stačí jen, aby byli připojeni na vnitřní policejní síť a měli zpřístupněný spis. Pak si můžou spis prostudovat a objektivně vyslovit svůj názor. Tento postup je zvláště výhodný u zvlášť závažných trestných činů, kde odborná konzultace k věci je potřebná a není možné z časových důvodů se dostavit přímo na místo, kde se spis zpracovává. Při praktickém používání tohoto systému jsem zjistil, že chybí celorepublikové používání jednotného ETŘ, což je limitováno i technickým vybavením. V současné době systém běží samostatně v rámci jednotlivých krajů. Dále je zde nedostatečná funkce některých formulářů, kterým chybí prakticky využitelné položky. Ne vždy co nabízí formulář je potřebné při praktické činnosti. Dále jsem při praktickém používání popisovaného systému zjistil, že ne vždy jsou plně využívány jeho veškeré funkce a proto jsem po dohodě s vedoucím služebním funkcionářem vypracoval tuto práci, která by měla pomoci začínajícím pracovníkům při práci s tímto systémem. Po prostudování tohoto materiálu by měl začínající pracovník se zařazením ve spisové službě Městského ředitelství Policie České republiky v Ostravě pochopit strukturu systému, jeho činnost a využití. Měl by pochopit praktické základy práce s tímto systémem a rozšířit si obzory i o teoretickou oblast informačních systémů v rámci celé veřejné správy. Při čtení této práce by se mu do rukou měla dostat praktická příručka k uplatňování zásad pro používání informačních systémů v rámci instituce Policie ČR.

Závěr

Veřejná správa jako moderní struktura jednotlivých institucí spravujících věci veřejné by měla jít lidem naproti a usnadňovat jim život. Moderní struktura by měla využívat všech dostupných moderních prostředků, které současná společnost nabízí a tyto účelně používat v oblasti služeb pro lidi, kterým by měla vycházet vstříc. Uvědomit si, že lidé jsou plátci daní a službu veřejné správy si platí pro potřeby využití. Není tomu tak, že občan instituci nezajímá a měl by se přizpůsobit. Instituce veřejné správy by také měly pracovat tak, aby účelně vynakládaly potřebné prostředky a pracovaly úsporně, k čemuž bezesporu dochází při používání moderních informačních systémů. Při dnešním technologickém pokroku, není problém, aby potřebné informace byly čerpány, předávány a využívány účelně prostřednictvím moderních informačních technologií, které jsou využívány v rámci veřejného sektoru.

Při zpracování této práce jsme se zaměřili na moderní informační technologie ve veřejné správě. U těchto moderních informačních technologií byla zjišťována jejich aplikaci do praxe, cílem práce bylo analyzovat moderní informační systémy v konkrétní instituci ve veřejné správě, respektive v Policii České republiky a zjistit možnosti dalšího rozvoje těchto systémů.

V první části se práce zaměřuje na teoretickou rovinu informačních technologií. Provádí se zde teoretický popis informačních technologií, jejich vznik, vývoj, účelovost a využití. Ve druhé části je práce zaměřena na veřejnou správu. Popisuje se zde oblast veřejné správy s uvedením konkrétních moderních informačních technologií v tomto sektoru. V závěru teoretické části se práce zabývá bezpečnosti při čerpání a zpracovávání datových toků s poukázáním na legislativní rámec bezpečnostní politiky.

V empirické části bylo zjišťováno jaké konkrétní informační technologie se používají ve veřejné správě v rámci konkrétní instituce při Městském ředitelství Policie České republiky v Ostravě. Zaměřujeme se na popis využívaných informačních technologií, provádí se zde popis těchto technologií. Byla popsána účelovost, funkčnost a praktické využívání těchto technologií. Následně byla provedena analýza této instituce, zda dochází k aplikaci moderních informačních

technologií do praxe. Byla zde řešena otázka bezpečnostních prvků v oblasti využívání informačních systémů. Závěrem je zde provedeno zhodnocení využívání informačních systémů v rámci instituce MŘ PČR s návrhy možných doporučení pro jejich kladný budoucí vývoj.

SEZNAM LITERATURY A PRAMENY

Knihy

BUREŠ, M., MORÁVEK, A., JELÍNEK, I. *Nová generace webových technologií.* Praha : Vox a.s., 2005. ISBN 80-86324-46-X.

GÁLA, L., POUR, J., ŠEDIVÁ, Z. *Podniková informatika, 2. Přepracované a aktualizované vydání*. Praha : Grada Publishing, 2009. ISBN 978-80247-2615-1.

HALÁSEK, D. *Veřejná ekonomika. 2. vydání, přepracované.* Opava : Optys, 2007. ISBN 80-85819-60-0.

HALÁSKOVÁ, M. *Veřejná správa v České republice a zemích EU. Ostrava.* Ostrava : VŠB TU, Ekonomická fakulta, 2006. ISBN 80-248-1266-5.

HÄBERLE, H. *Průmyslová elektronika a informační technologie.* Praha : Europa - Sobotáles, 2004. ISBN 80-86706-04-4.

HEBRYCH, D a kol., *Správní právo – obecná část, 7. Vydání*. Praha : C.H. BECK, 2009. ISBN 978-80-7400-049-2.

ŠTĚDROŇ, B. *Manažerské řízení a informační technologie*. Praha : Grada, 2006. ISBN 80-247-2052-3.

TOTH, P. *Informační systémy státní správy a územní samosprávy*. Praha : VŠE, Fakulta národohospodářská, 1993. ISBN 80-7079-855-6.

TVRDÍKOVÁ, M. *Aplikace moderních informačních technologií v řízení firmy*. Praha : Grada, 2008. ISBN 978-80-247-2728-8.

Internetové zdroje:

Archiv stránek Ministerstva vnitra České republiky, (online) 2010 (cit. 15.3.2010). Dostupné z WWW:http://www.czechpoint.cz/web/

Archiv stránek Veřejné správy České republiky, (online) 2010 (cit. 12.3.2010). Dostupné z WWW: ISVS.CZ

Archiv stránek Portálu veřejné správy České republiky, (online) 2010 (cit. 10.3.2010). Dostupné z WWW: http://portal.gov.cz/wps/portal/_s.155/6966/place

Archiv stránek Ministerstva vnitra České republiky, (online) 2010 (cit. 10.2.2010). Dostupné z WWW: http://www.datoveschranky.info/

Archiv stránek Ministerstva vnitra České republiky, (online) 2010 (cit. 10.2.2010). Dostupné z WWW: http://www.mvcr.cz/

Zákony a jiné dokumenty:

Zákon č. 513/1991 Sb., obchodní zákoník.

Zákon č. 140/1961 Sb., trestní zákon.

Zákon č. 306/2009 Sb., trestní zákoník.

Zákon č. 273/2008 Sb., o Policii České republiky.

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Zákon č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

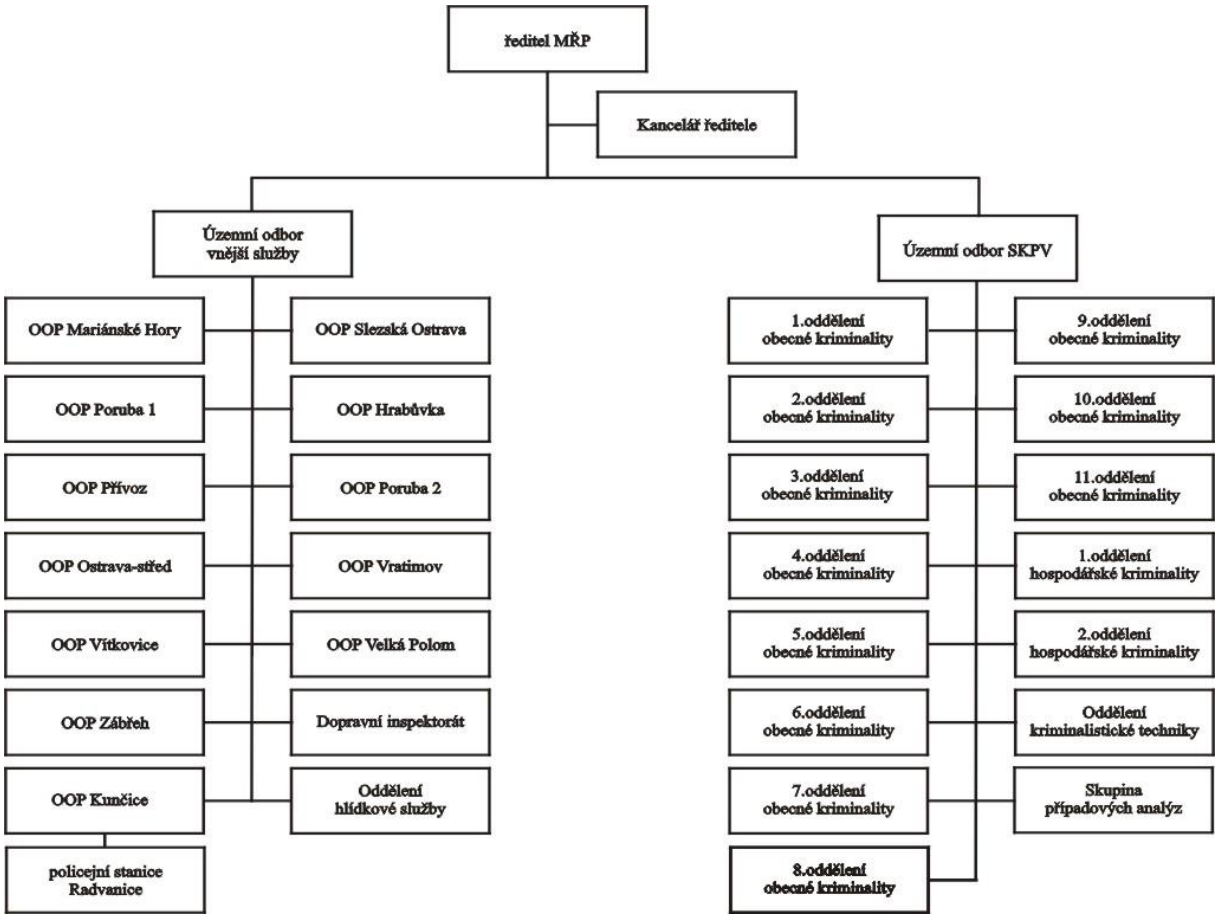
Zákon č. 151/2000 Sb., o telekomunikacích, ve znění pozdějších předpisů.

Zákon č. 227/2000 Sb., o elektronickém podpisu.

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

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.

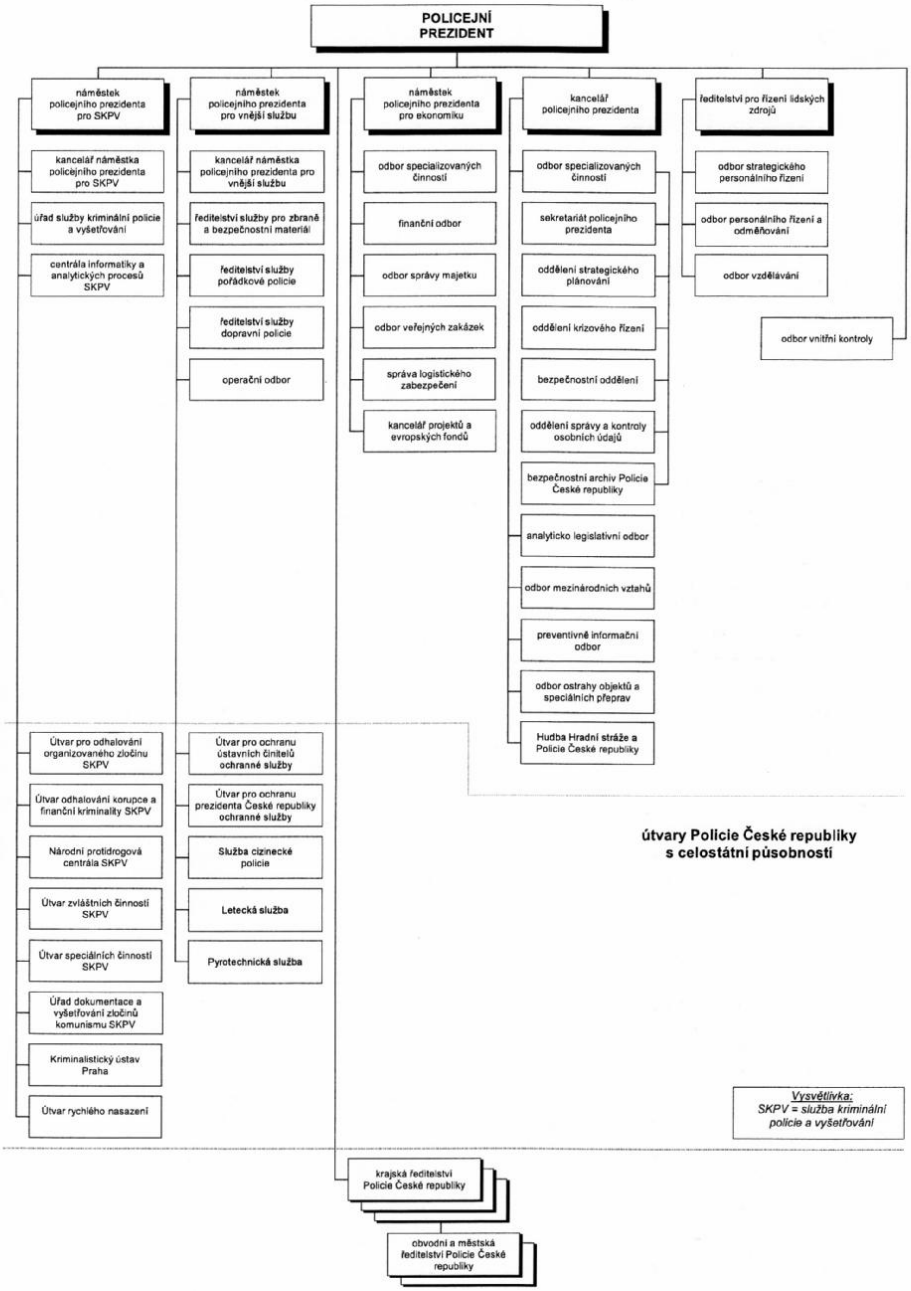
PŘÍLOHY:

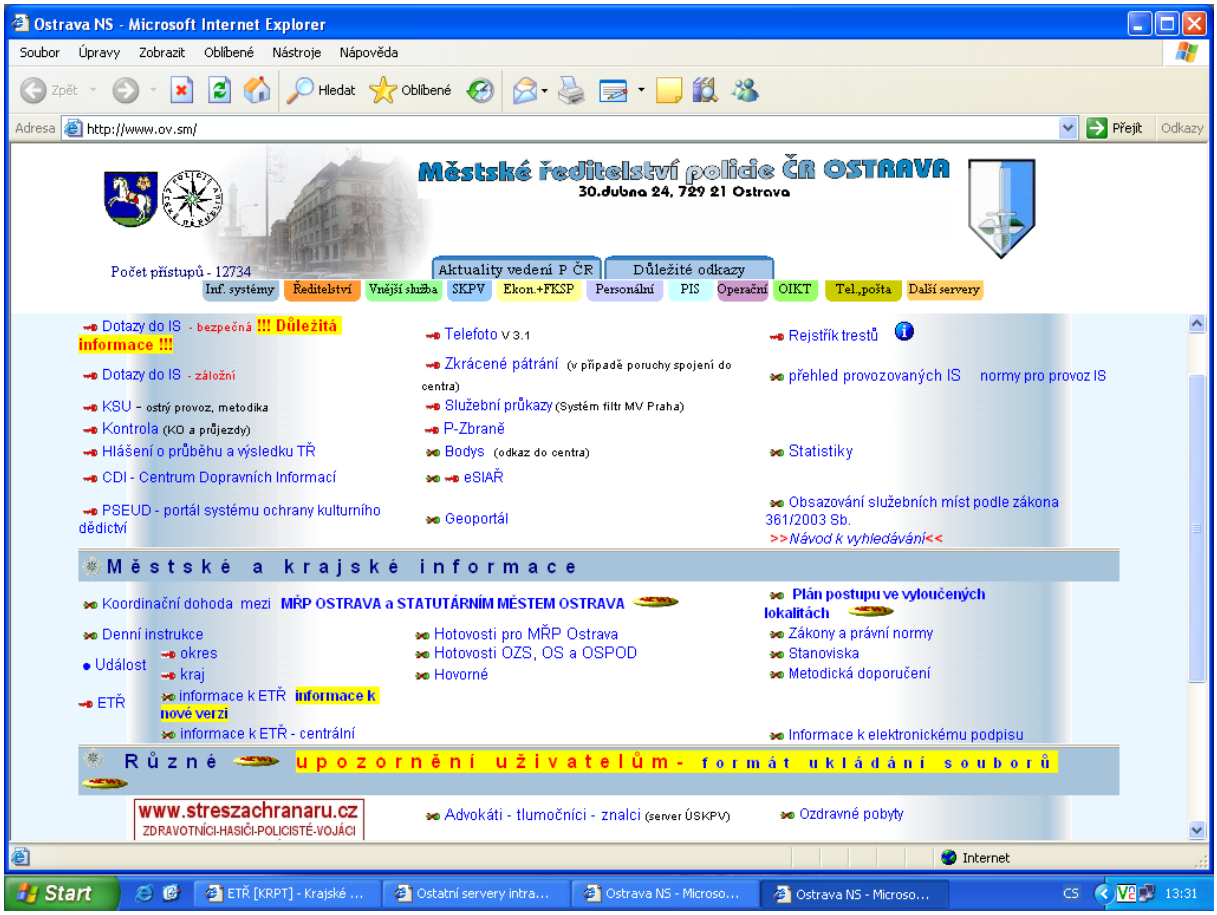


Organizační struktura jednotlivých oddělení v rámci struktury Městského ředitelství Ostrava Policie České republiky a v rámci celé ČR.

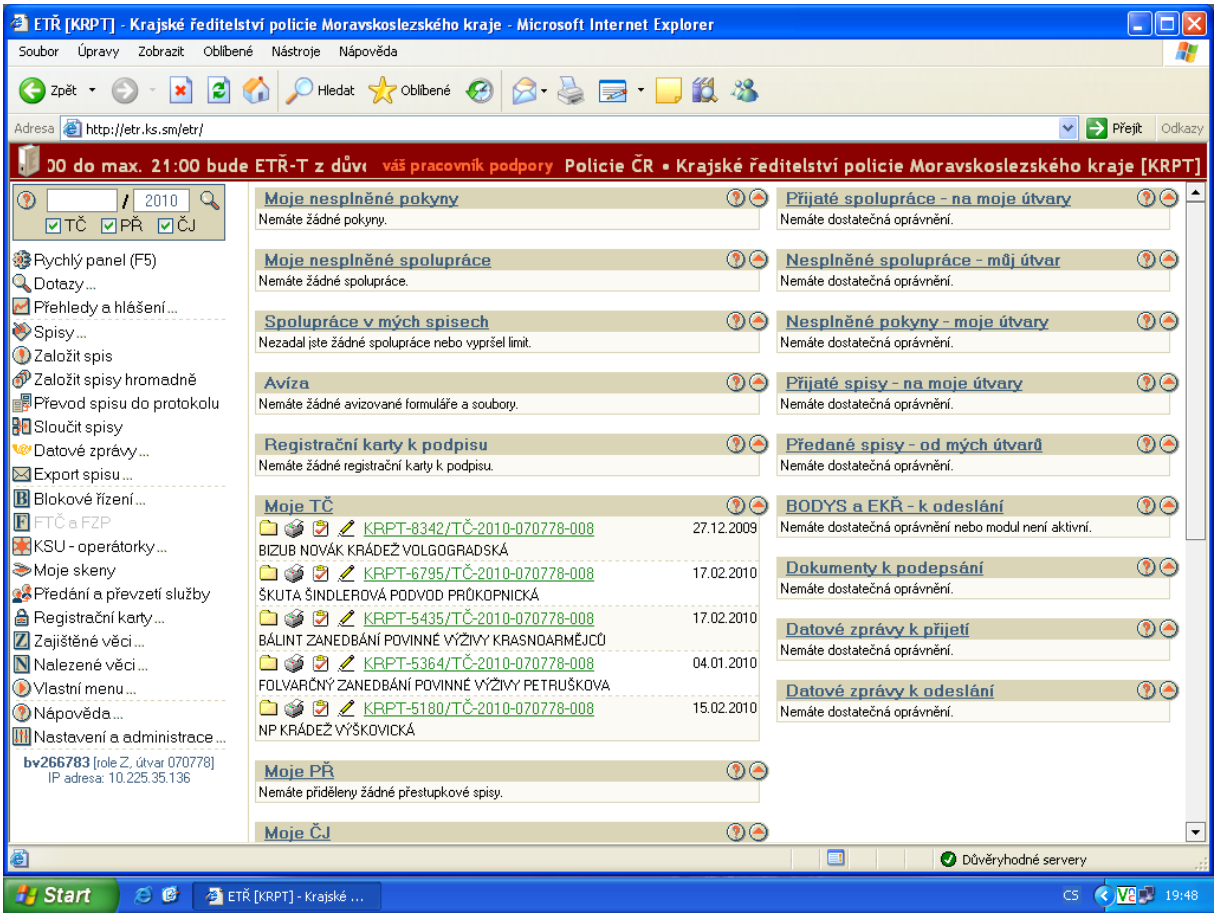
Příloha č. 2 k RPP č. 226/2008

Organizační schéma Policie České republiky

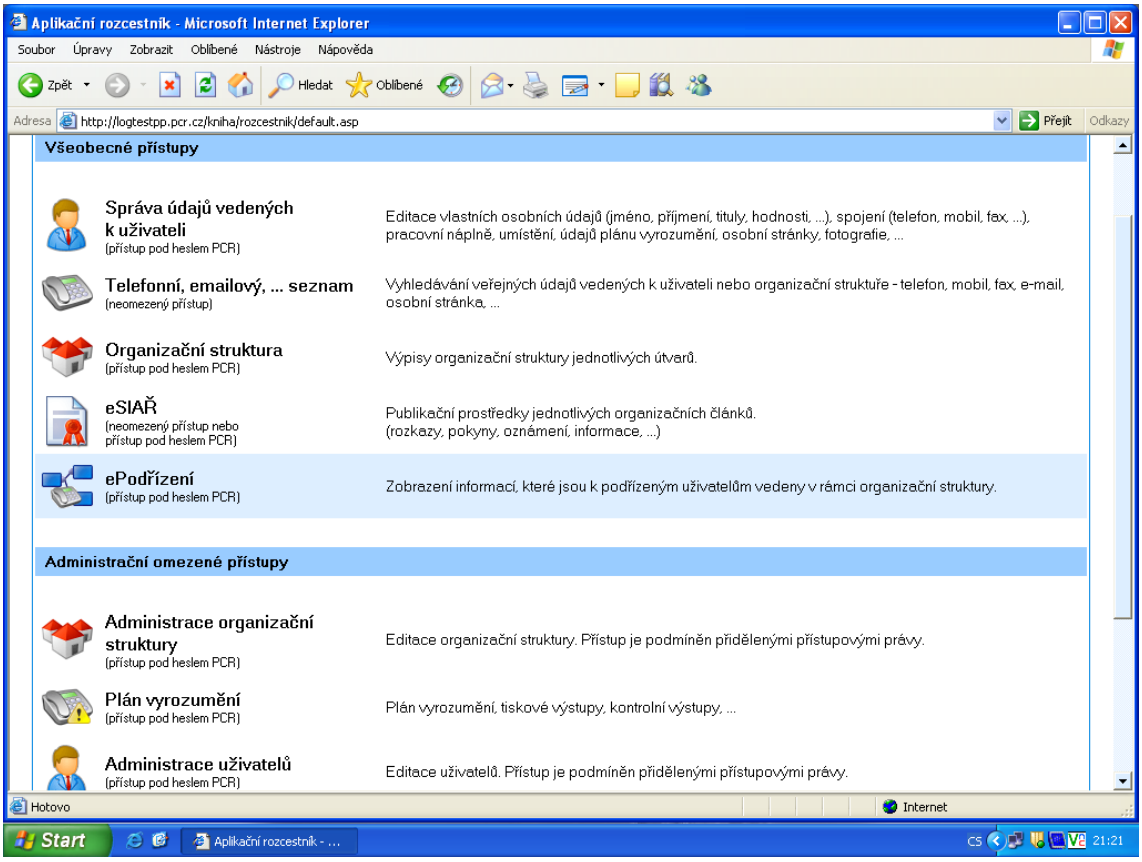




Ukázka panelu informačního systému pro pracovníky Městského ředitelství Policie České republiky v Ostravě.



Ukázka informačního panelu Elektronického trestního řízení.



Ukázka informačního panelu eSIAŘ.

ANOTACE

Jméno a příjmení:	Bohdan Velička
Katedra:	Ústav pedagogiky a sociálních studií
Vedoucí práce:	RNDr. Evžen Růžička, CSc.
Rok obhajoby:	2010

Název práce:	Moderní informační technologie ve veřejné správě
Název v angličtině:	Modern Information Technology in Public Administration
Anotace práce:	Práce obsahuje přístupy k pojetí moderních informačních technologií používaných ve veřejné správě se zaměřením na oddělení Městského ředitelství Policie České republiky.
Klíčová slova:	Informatika, moderní technologie, komunikační systémy, veřejná správa, Policie České republiky, elektronické soudní řízení.
Anotace v angličtině:	Bachelor thesis includes the approaches of modern information technologies which are being used in public administration with a focus on the department of the Municipal Police Directorate of the Czech Republic.
Klíčová slova v angličtině:	Information science, modern technology, communication systems, public administration, the Police of the Czech Republic, e-proceedings.
Rozsah práce:	56 s
Jazyk práce:	český jazyk