VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, O. P. S.

Žižkova 6, 370 01 ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

INFORMAČNÍ SYSTÉMY POLICIE ČESKÉ REPUBLIKY A JEJICH APLIKACE

Autor práce: Jakub Šťástka

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinované studium

Vedoucí práce Mgr. et Bc. Josef Kříha

Katedra: Katedra právních oborů a bezpečnostních studií

2010

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně s využitím uvedených pramenů a literatury.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna ke studijním účelům.

Jakub Šťástka

Děkuji vedoucímu bakalářské práce Mgr. et Bc. Josefu Kříhovi za metodické vedení, rady a připomínky k bakalářské práci.

Obsah

ÚVOD

V této bakalářské práci se zabývám samotným „Informačním systémem“ jak z pohledu teorie, kde se snažím popsat samotnou historii vývoje informačních systémů ve světě i v České republice a posléze u Policie České republiky, tak funkční a to zejména rozdělením do kritérií s využitím u Policie České republiky. Je neoddiskutovatelným faktem, že informační systémy jsou v současné době nepostradatelnou součástí různorodých rozmanitých policejních činností.

Důvodem výběru zvoleného tématu je jeho aktuálnost a téma jako takové není až tak známé a vlastní čtení třetí, nezainteresovanou osobou z civilního sektoru by mohlo přinést jí užitečné a dosud neznámé poznatky a tímto i rozšířit obzory vědění.

Vzhledem k tematickému zaměření studijního oboru „Bezpečnostně právní činnost“, který je zabezpečován Vysokou školou evropských a regionálních studií, o. p. s., je základní myšlenka zpracována zejména z právního hlediska a téma se tedy citelně dotýká jednotlivých zákonů, které se opírají o sféru trestně, ale i správně právní konsekvence využití informačních systémů v praktické policejní činnosti a poukazuje na nezbytnosti využívání informačních systémů a technologií orgány Policie České republiky.

Bakalářská práce si ve svém maximálním postihu rovněž klade za dílčí cíl shrnout veškeré znalosti a poznatky z oblasti informačních systémů a technologií v souvislosti s Policií České republiky a jelikož se jedná o teoretickou práci, snaží se tedy detekovat praxeologické výstupy dané problematiky.

1 CÍL A METODIKA BAKALÁŘSKÉ PRÁCE

Cílem této bakalářské práce je objasnit funkci informačních systémů aktuálně využívaných u Policie České republiky v širším smyslu. Stanovit a specifikovat možnost a diverzifikaci využití informačních systémů v rámci specifické činnosti orgánů Policie České republiky. V užším slova smyslu definovat a určit kladné a záporné stránky jednotlivých informačních systémů z pohledu možností příslušníka základního útvaru Policie České republiky. Navrhnout možné systémové změny a alternativní způsoby využití informačních systémů Policie České republiky při zajištění taxativně stanovených úkolů Policie České republiky uvedených v aplikaci ustanovení § 2 zákona č.273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů souvisejících např. se zabezpečením bezpečnosti osob a majetku, ochranou veřejného pořádku, předcházení páchání trestné činnosti, dokumentací různých forem trestné činnosti, jednotlivých jevů a fází trestných činů.

V první části této bakalářské práce jsem považoval za důležité definovat, co je vlastně „informační systém“, jak a kde začal vznikat, jeho vývoj do dnešních dnů a snaha k nahlédnutí do dnů či let budoucnosti a pokusit se definovat i možnosti ve využití vlastních informací Policie České republiky vkládaných do informačních systémů.

Vlastní práci jsem rozdělil do několika částí, a to rozdělení a využitelnost vlastních informačních systémů jak v celosvětovém měřítku, tak u samotné Policie České republiky v rámci jednotlivých Územních odborů, jejich vývoj, vymezení jednotlivých neutajených informačních systémů, jejich kladné a záporné stránky, teze možných úprav a možné pohledy do budoucnosti. V práci dále budou uplatněny výzkumné metody řízeného rozhovoru, anketa a potřebné příklady k objasnění nejen exkursivním způsobem vymezeného momentálního, ale i minulého stavu a budoucnosti informačních systémů a technologií u Policie České republiky. Bohužel v této práci nelze dostatečně a kvalifikovaně použít výzkumnou metodu dotazníkového šetření, zejména z důvodu nedostatku kvalifikovaného výběru respondentů. Jednotlivé přístupy k informačním systémům jsou samozřejmě založeny na stupni oprávnění přístupů, tzv. škálu oprávnění přístupů, kdy každý jednotlivý stupeň oprávnění z této škály je ještě definován

samostatně a individuálně. S tímto tato skutečnost zcela bezesporu souvisí s určitou omezeností kvalifikovaného výběru respondentů pro případné uplatnění a využití metody tzv. dotazníkového šetření.

2 INFORMAČNÍ SYSTÉMY A HISTORICKÝ VÝVOJ

2.1 Informační systém

Informační systém je systém pro sběr, udržování, zpracování a poskytování informací a dat.

Příkladem informačního systému může být například kniha docházek, telefonní seznam nebo účetnictví. Systém nemusí být nutně automatizovaný pomocí počítačové techniky, ale může být i v papírové podobě, nicméně v dnešní době se ve více jak 99 % hovoří o automatizovaném informačním systému a při samotném slově „informační systém“ se toto v myslích lidí spojuje s počítačem či internetem.

Informační systém potřebuje nutně jak ke sběru, udržování, zpracování a poskytování dat „informace“. Informacemi míníme sdělení, které odstraňuje nevědomost nebo nejistotu, daty pak míníme jakékoliv zaznamenané poznatky či fakta. Jako zvláštní pojem zde vystupuje také „znalost“ představující zobecnění poznání určité části reality. Informace jako také je ale možné také chápat jako data s nějakým přidaným významem (data + význam, tj. dne 20. prosince 2009 + trestný čin dle § 238 trestního zákona). Samotnou informací je údaj – množné číslo data, ke kterému si člověk přiřadí nějaký význam. K rozvoji informací napomáhají také znalosti nových technologií a podobně.

Výše je uvedeno, že více jak z 99 % se mluví o informačním systému ve spojitosti s počítačovou technikou a internetem. Z pohledu internetu, tedy celosvětovým systémem navzájem propojených počítačových sítí, ve kterých mezi sebou počítače komunikují pomocí rodiny protokolů TCP/IP. Společným cílem je tedy bezproblémová komunikace a výměna dat. První vizí počítačové sítě nalezneme v povídce z roku 1945. V roce 1962 vzniká projekt počítačového průzkumu agentury ARPA, která v roce 1969 vytvořila experimentální síť ARPANET, až v roce 1987 vzniká samotný pojem „Internet“, kdy je v síti propojeno více jak 27.000 počítačů. V roce 1992 vstupují vládní instituce v USA – konkrétně Bílý dům na tzv. pódium internetu. O dva roky déle internet komercializuje a v roce 2006 má připojených více jak miliardu uživatelů. V

České republice v listopadu 2008 mělo připojení k internetu 32 % domácností a 90 % domácností mělo možnost připojení k internetu V době vývoje internetu se vyvíjí také počítačová technika a také vznikají nové informační systémy, které se postupně vyvíjí až do dnešní podoby.

2.2 Informační systémy PČR a jejich obecné vymezení

Informační systémy Policie České republiky, které nepodléhají utajení jsou systémy využívané prostřednictvím výpočetní techniky a sítě intranet, která dubluje síť internet, ale je sítí uzavřenou, tedy nepropojenou s veřejnou sítí internet. Informační systémy jsou užívané všemi službami Policie České republiky pro konkrétní potřebu. Služby Policie ČR má složitou hierarchii, ale jednoduchým klíčem ji lze rozdělit do několika článků a to;

- Policejní prezidium, jako článek nejvyšší,
- Službu Pořádkové policie,
- Službu Dopravní policie,
- Službu Kriminální policie a Vyšetřování,
- Odbor vnitřní kontroly (Inspekce PČR).

Dále jsou útvary rozděleny na útvary s celorepublikovou působností, kdy se jedná o;

- Kriminalistický ústav Praha,
- Letecká služba,
- Národní protidrogová centrála SKPV,
- Služba cizinecké policie,
- Úřad dokumentace a vyšetřování zločinů komunismu SKPV,
- Útvar odhalování korupce finanční kriminality SKPV,
- Útvar pro odhalování organizovaného zločinu SKPV,
- Útvar pro ochranu prezidenta ČR,
- Útvar pro ochranu ústavních činitelů,

- Útvar rychlého nasazení,
- Útvar speciálních činností SKPV,
- Útvar zvláštních činností SKPV.

Dále se jedná o útvary s omezenou (místní) působností a to;

- v rámci kraje – krajská ředitelství,
- v rámci okresu – územní odbory,
- v rámci obvodu – obvodní oddělení a železniční oddělení,
- v rámci místa – hlídková služba v rámci např. Českých Budějovic.

Všechny tyto služby využívají jednotlivé IS dle svých potřeb a oprávnění. U Policie České republiky se IS rozdělují na celoplošné, neboli celorepublikové a místní, např. krajské či okresní. Většina z dnešních IS se provozuje přes webové rozhraní prostřednictvím webového prohlížeče, u policie většinou Microsoft Internet Explorer 6 a 7 dle možností jednotlivé počítačové techniky. Jsou ale i informační systémy provozované lokálně na jednotlivých počítačích, které se dávkově, např. mailem doplňují např. jednou za 24 hodin a nebo existují informační systémy na bázi DOS verze, přičemž u těchto je omezené využití v počtu uživatelů v jednom okamžiku připojení a omezené množství přenášených dat systémem.

2.3 Historická retrospektiva, vývoj informačních systémů u Policie České republiky

V letech před listopadovou revolucí, tedy déle jak před 20-ti lety Policie, tehdy Sbor národní bezpečnosti (SNB) využívala výpočetní techniku sporadicky a to jen při např. znaleckých zkoumáních nebo expertízách, nicméně v této době se nedá říci, že by Policie (SNB) využívala nějaké s počítačem spojené informační systémy, vše bylo strojově tištěno a publikováno např. knižně. Spisová služba se vedla ve sběrném archu, nic tedy nenasvědčovalo pozdějšímu využití počítačové techniky, a tedy šlo o využívání informačních systémů, ale např. psaných a ručně zakládaných, tříděných a

revidovaných. V době okolo roku 1998 dochází k zavádění PC techniky na jednotlivé pozice, ale jedná se pouze o ojedinělé případy. Počítačem v té době je vybaveno pouze oddělení na operačních střediscích, u velitelů a vedoucích jednotlivých skupin, na stálých službách jednotlivých výše popsaných struktur policie a v té době, přestože se ještě vše dokumentuje tištěnou či psanou formou v několika výtiscích a spisový řád se vede „dvojmo“ na sběrném archu, již vznikají první informační systémy spojené s výpočetní technikou. Počítač u policie slouží v této době na informace týkající se denního nápadu v jednotlivých teritoriích[1]. Jednoduchá vkládání svědčí i o jednoduchosti informačního systému. Základní článek, dozorčí Obvodního oddělení vkládá informaci o události, která se stala a má být dle předpisu evidována. Informace v té době se skládá z informace, pod jakým číslem jednacím je událost vedena, co se stalo, kde se to stalo, v jaké době se to stalo, komu se to stalo, tedy dle kritérií kriminalistických otázek. Tato informace prostřednictvím zašifrované dávky byla zaslána na operační středisko, kde byla zařazena do jednoho z prvních Informačních systémů Policie ČR – UDÁLOST. Zajímavostí je, že tento informační systém s drobnými úpravami funguje do dnešní doby, i když již není založen na dávkovém upgradu, ale na on-line verzi a je dostupná na jakémkoliv počítači v rámci síťového připojení intranet Policie ČR. Když se ale vrátím zpět do jakékoliv doby před realizací jakéhokoliv informačního systému je zapotřebí zmínit organizaci řízení tvorby návrhu a jeho fáze.

3 TVORBA INFORMAČNÍCH SYSTÉMŮ

tvorbě informačních systémů se dá rozdělit do několika bodů;

- úvodní studie,
- rozbor zadání,
- analytické modelování,
- systémový design,
- objektový design,

[1] ČR: Policie České republiky, Okresní ředitelství České Budějovice, OOP České Budějovice (empirický zdroj)

- implementace,
- zkušební provoz,
- nasazení do ostrého provozu

Hlavním artefaktem jsou případy užití nebo také tzv. „use cases“ – modely jednání. Základními prvky jsou;

- aktér
- scénář
- reakce

3.1 Objektový model

„Model spolupráce je dalším artefaktem, který vzniká na základě dalších případů užití. Hledáme zde první náznaky tříd, odpovědností a vztahů. To pak ústí v objektový model, který již přesně zachycuje celý systém, vztahy mezi objekty či hierarchii dědění.

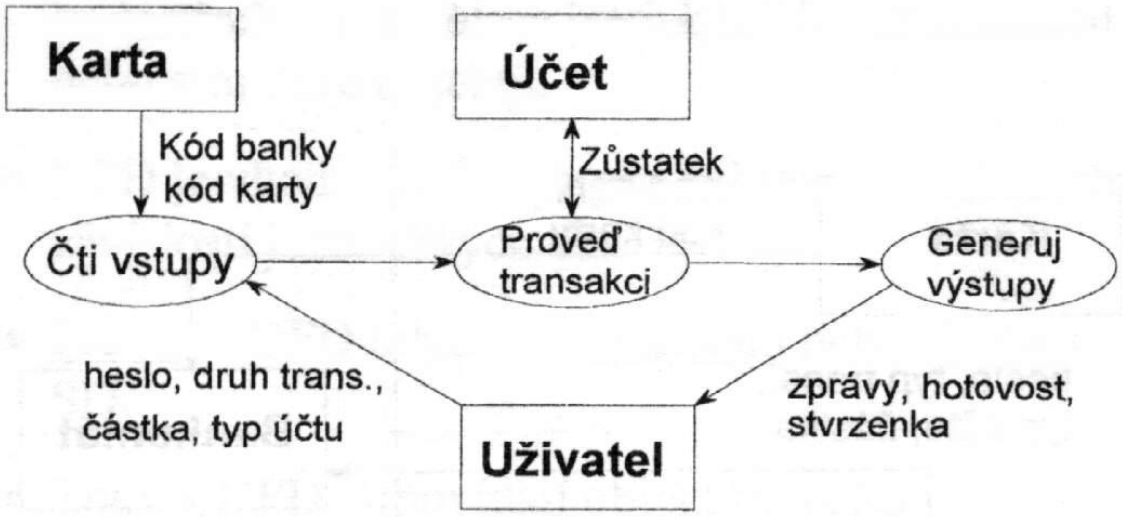
.

Obrázek č. 1 – objektový model[2]

[2] Reboot.cz (online) 2009 (cit. 2009-11-19 12:35 hod.). Dostupný z WWW: http://reboot.cz/obrazky/objmod2.jpg

3.2 Funkční model

Funkční model poskytuje kontrolní pohled na vytvářený systém, de facto standardem je zde DFD model, jež poskytuje snadné grafické vyjádření propojitelné s datovým modelem. DFD model je hierarchický, to znamená, že procesy se dají postupně zjemňovat. Každý proces tedy obsahuje „vnořený" diagram, a tak dále až po takzvané listové procesy, které jsou nedělitelné. Každý proces v DFD obsahuje textový opis, popis omezení a také dostatečné informace."[3,4]



Obrázek č. 2 – funkční model [5]

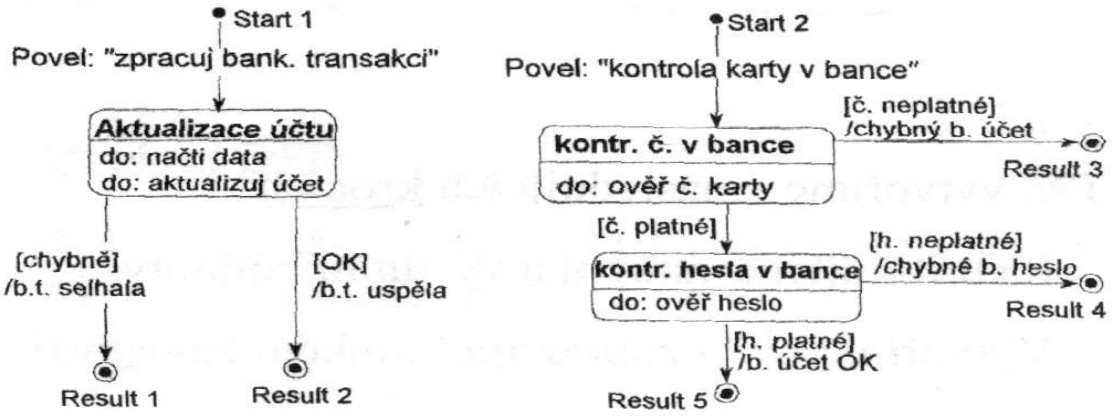
[3] Otevřená encyklopedie WIKIPEDIA (online) 2009 (cit. 2009-11-19 12:35 hod.). Dostupný z WWW: http://cs.wikipedia.org/wiki/Informa%C4%8Dn%C3%AD_syst%C3%A9m

[4] Molnár Z., Automatizované informační systémy, 1. vydání, Praha: Vydavatelství ČVUT, 2000, 52 s, ISBN: 80-01-02269-2

[5] Reboot.cz (online) 2009 (cit. 2009-11-19 12:37 hod.). Dostupný z WWW: http://reboot.cz/obrazky/dfd.jpg

3.3 Dynamický model

„Dynamický model přispívá k pochopení změn v systému. Možné popisy jsou například slovní scénáře, grafické scénáře, mapy událostí nebo stavové tabulky a diagramy.“[6]



Obrázek č. 3 – dynamický model[7]

3.4 Architektura informačních systémů

„Velmi důležitým hlediskem je volba architektury. Téměř výhradně se používá 3vrstvá architektura;

- *presentační (interakce s uživatelem),*
- *funkční (vlastní aplikace, bezpečnost, propojení se světem, kontrola, ...),*
- *datová (vlastní data).*

Důležitá je i bezproblémová integrace informačního systému, která má dvě hlediska: vnitřní, kde jde o proškolení pracovníků, nastavení prostředí a podobně, a vnější, kde se jedná zejména o zákazníky a dodavatele. Je nutné si uvědomit, že zadavatel implementace IS bude hledět na:

- *základní údaje (nejen samotného IS, ale také dodavatele),*
- *architekturu (zda-li mu bude vyhovovat),*
- *reference (po ČR i ve světě),*

[6] Reboot.cz (online) 2009 (cit. 2009-11-19 12:39 hod.). Dostupný z WWW: http://reboot.cz/howto/programovani/objektove-orientovane-metody-analyzy/articles.html?id=102

[7] Reboot.cz (online) 2009 (cit. 2009-11-19 12:48 hod.). Dostupný z WWW: http://reboot.cz/obrazky/dfd.jpg

- *provozní prostředí (databázová platforma),*
- *vývojové prostředí (CASE nástroje),*
- *dokumentace*
- *doplňující služby (podpora, školení),*
- *standardy, specifikace, certifikace (audity, ISO-9000),*
- *flexibilita (možnost přizpůsobení).“*[8]

3.5 Implementace informačních systémů

„Implementaci informačního systému předchází většinou důkladná analýza požadavků firmy i samotných procesů, které se ve společnosti používají. Většina systémů se implementuje jako tzv. datové sklady, což je architektura (obvykle založená na SŘBD), jež transformuje operativní data do jiné podoby, u které se bere ohled například na čas a rychlost následných dotazů. Tato data se nemění, mohou se transformovat z více zdrojů a jsou aktualizována v časových intervalech. Nad nimi se dělají statistiky či analýza.“[9]

4 SOUČASNÝ STAV INFORMAČNÍCH SYSTÉMŮ U POLICIE ČR

V dnešní době je u Policie ČR vedeno na několik desítek informačních systémů, které nepodléhají utajení a mnoho dalších, o kterých se v této bakalářské práci nelze zmiňovat. Nicméně celkově lze říci, že v roce 2009 je většina systémů provozována on-line, tedy např. při doplnění informace o kontrole vozidla na kontrolním bodě v Českých Budějovicích a zadání této informace prostřednictvím PC do datového skladu určitého informačního systému, je ihned ve stejném okamžiku tato informace dostupná on-line kdekoliv v intranetové síti PČR. Bohužel v této době musím říci, že se jedná o většinu informačních systémů a ne všechny. Stále jsou systémy, které se doplňují dávkově. Když do tohoto položí policista dotaz, musím čekat i několik dní na odpověď, nicméně o tomto problému se budu zmiňovat v další části mé bakalářské práce.

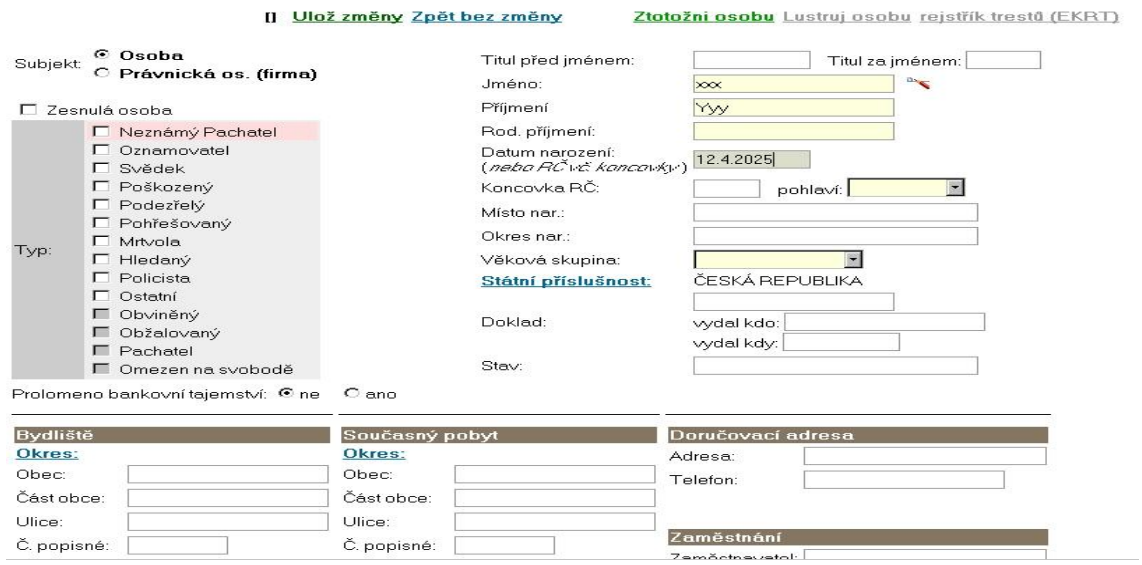
[8] Otevřená encyklopedie WIKIPEDIA (online) 2009 (cit. 2009-11-19 12:50 hod.). Dostupný z WWW: http://cs.wikipedia.org/wiki/Informa%C4%8Dn%C3%AD_syst%C3%A9m
[9] Otevřená encyklopedie WIKIPEDIA (online) 2009 (cit. 2009-11-19 11:30 hod.). Dostupný z WWW: http://cs.wikipedia.org/wiki/Informa%C4%8Dn%C3%AD_syst%C3%A9m

4.1 Dělení informačních systémů

Pokud bych měl rozdělit informační systémy využívané policisty v rámci služby či občanskými pracovníky využívané v rámci své pracovní náplně, činil bych takto. Jsou informační systémy, které plní funkci pouze informační, tedy dotazovací a tedy tyto informační systémy jakoby „sahají“ do databáze jiných informačních systémů, které jsou pro ně za určitých podmínek dostupné či přístupné. V tomto případě se může jednat třeba o ztotožňování osob při zadání pouze jména, příjmení a data narození ve spisovém materiálu elektronického spisu v informačním systému „Evidence trestního řízení“, dále ETŘ.

Obrázek č. 4, který je znázorněn níže dokladuje tu skutečnost, že Informační systém, v tomto případě zmiňované „ETŘ“ při zadání imaginární osoby jménem X**xx,** příjmením **Yyy** a datem narození **12.4.2025** při kliknutí hypertextového odkazu „Ztotožni osobu“ dokáže logem, který se archivuje v databázi šáhnout do jiného skladu jiné databáze, v tomto konkrétním případě databáze „Centrální registr obyvatel“, dále CRO a v případě, že tato osoba v registru existuje, tuto ztotožnit a doplnit ostatní volná pole, které jsou znázorněna na obrázku.

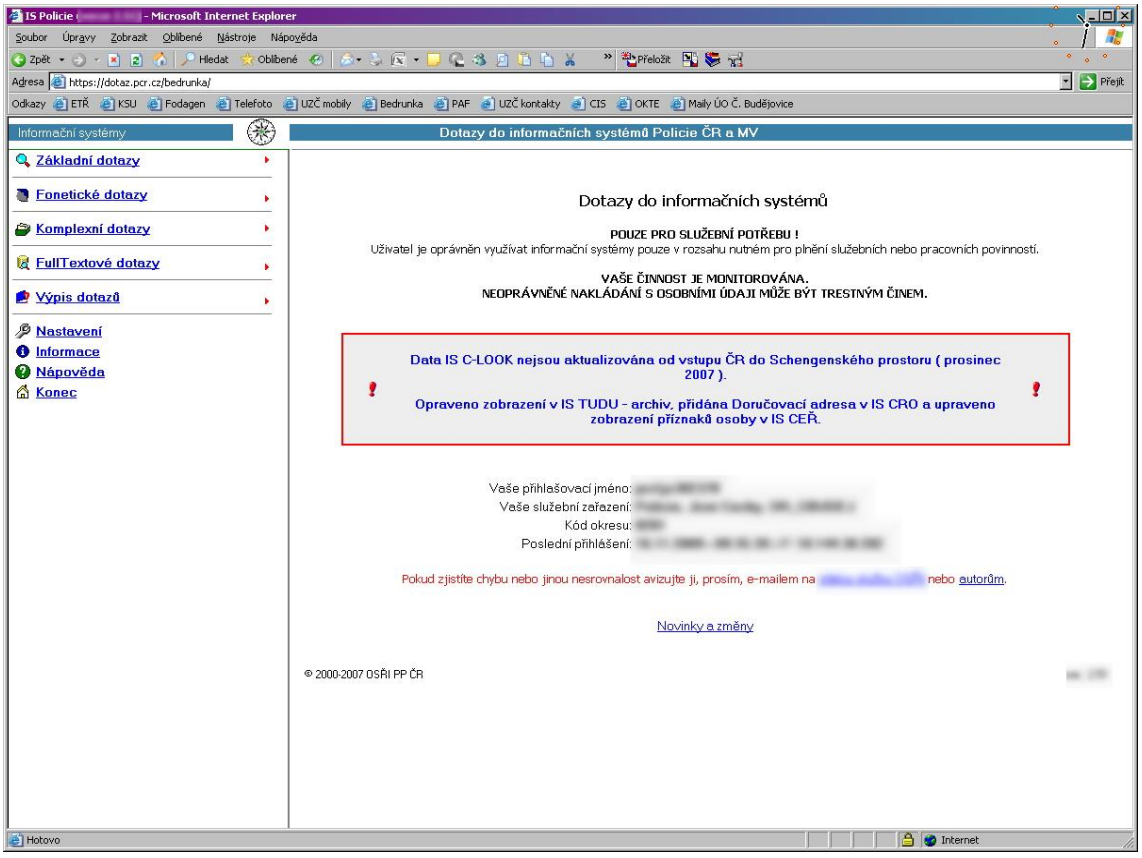
Obrázek č. 4 – část obrazovky informačního systému ETŘ, záložka osoba



Je samozřejmostí, že v databázi CRO nejsou evidovány údaje, jako je telefonní číslo či zaměstnání. Toto jsou nepovinné položky, které je možné a vhodné vyplnit dodatečně po automatickém ztotožnění, ale jen se souhlasem osoby, která je do systému vyplňována a která tyto údaje uvedla třeba do policejného výslechu či úředního záznamu.

4.2 Zprostředkovatelské informační systémy

Mezi výše popsané informační systémy, které slouží jen jako zprostředkovatelé informací či výstupů z jiných datových skladů patří jednoznačně informační systém IS POLICIE.



Obrázek č. 5 – Informační systém IS Policie – úvodní strana

V tomto informačním systému lze podle oprávnění 1 – 5, kdy 1 znamená základní dotazy a 5 znamená nejvyšší oprávnění na fulltextové dotazy „sahat“ zadáním dotazů do informačních systémů jako je CRO, Centrální registr vozidel CRV, pátrání po

osobách PATROS, pátrání po motorových vozidel PATRMV, evidencí zbraní, evidencí zbrojních průkazů, Schengenského informačního systému, seznamu odcizených uměleckých děl SEUD, kontroly osob a motorových vozidel – KO, průjezdů přes hraniční přejezdy Look, evidenci dopravních nehod Z-EDN a podobně. Škála dotazů je velká a pravidelně se rozšiřuje o další informační systémy. Jak již bylo zmíněno, u oprávnění nižšího stupně může např. policista obvodního oddělení vznést dotaz na konkrétní osobu podle jejího rodného čísla či jména, příjmení a data narození. Již nemůže vznášet dotaz kombinovaný či fulltextový. Tento dotaz se vznáší v době, kdy policista neví, jak by se osoba mohla jmenovat, kdy se přesně narodila nebo v podobných případech, kdy nemá přesné údaje. Toto oprávnění má ale méně policistů, nejspíše proto, aby se předcházelo úniku informací či zneužití systému. Rozdělení do skupin však neplatí jen u systému IS Policie, ale u většiny dalších subsystémů či úplně odlišných systémů a pravidlo rozdělení je de facto u všech stejné;

- oprávnění 1 - 2 – pracovník obvodního oddělení, hlídkové služby apod.
- oprávnění 2 – 4 – pracovník Skupiny kriminální policie a vyšetřování
- oprávnění 4 – 5 – pracovník analytického pracoviště, operátor či operační důstojník

Samozřejmě, že toto výše uvedené rozdělení nelze paušalizovat, jelikož i na některých větších obvodních odděleních prvního tipu lze nalézt analytiky, kteří nepracují se všemi dostupnými informacemi, ale je možné je zařadit třeba do třídy 3. Toto ale je vždy alternativní a jak uvádím, nelze toto paušalizovat.

4.3 Informační systémy sloužící pro úschovu dat v datových skladech

Dalším rozdělením by se dalo říct, že nejen u Policie ČR, jsou informační systémy, které slouží pouze jako úschova dat pro systémy jako je např. „IS Policie“. Tyto informační systémy jsou jakýmkoliv způsobem plněny do datových skladů na centrálním serveru či lokálním PC a informace zde pouze leží a jen pokud se do nich jiný informační systém loguje, datový sklad je vydá k použití. Těchto systémů je poskromnu, ale přesto se najdou, nicméně pro účely této bakalářské práce je nemohu

jmenovat, většinou se jedná o systémy, které jsou v režimu utajení. Jen o jednom případu, který je veřejně publikovatelný vím a to je Evidence rejstříku trestů. Tento informační systém není provozován Policií ČR, ale pouze dotazem se lze dotázat do jiného datového skladu, kde jsou informace o trestní minulosti občanů. Lze z tohoto získat „výpis z rejstříku trestů“, „opis rejstříku trestů“ a další informace týkajících se trestů k daným konkrétním osobám. Je nutné podotknout, že tento informační systém slouží na této úrovni pouze jako podpůrný pro orgány činné v trestním řízení a do dnešní doby výstupy z něj někteří soudci či státní zástupci považují za nedostatečné a vyžadují od policistů originální kolkovaný doklad zaslaný poštou z oddělení „Rejstříku trestů“ v Praze.

4.3 Informační systémy „více-funkční“

Nejpoužívanější tip informačních systémů u Policie ČR je ten, který je zároveň plněn do datových skladů a zároveň z datových skladů informace vydává ve svém“originálním“ prostředí. Pro upřesnění uvedu několik nejpoužívanějších informačních systémů, které plní tuto úlohu. Jedná se o;

- Centrální registr obyvatel, dále CRO
- Centrální registr motorových vozidel, dále CRV
- Centrální registr zbraní, dále Zbraně
- Pátrání po osobách, dále PATROS
- Pátrání po motorových vozidlech, dále PATRMV
- Pátrání po uměleckých dílech, dále SEUD
- Kriminalisticky sledované události, dále KSU
- Evidence trestního řízení, dále ETŘ
- IS Telefoto
- IS Telefon
- IS Bankovka
- Evidence systémového řízení – publikační prostředek – E-Siař
- IS Událost

- MECHOS – virtuální centrální databáze mechanoskopických stop
- DROGIS – databáze tablet extáze
- IDENTOS – databáze depozitovaných lebek a kosterních nálezů
- atd. ...

4.3.1 Centrální registr obyvatel

Zajišťuje výdej dat pro orgány státní správy a rovněž slouží jako zdroj údajů pro jednotlivé složky policie.

- v registru obyvatel je vždy vedeno
    - jméno
    - příjmení, minulá příjmení
    - datum narození
    - koncovka rodného čísla
    - trvalé bydliště
    - rodinný stav
        - podružně číslo občanského průkazu
        - podružně číslo řidičského průkazu
        - podružně minulá hlášená bydliště
        - podružně odkazy na rodiče, děti a manžele či manželky
        - podružně vedena fotografie z občanského průkazu

4.3.2 Centrální registr motorových vozidel

Obsahuje všechna provozovaná i vyřazená motorová i nemotorová (přívěsy, návěsy atd. vozidla evidovaná v ČR, kterým jsou přidělovány státní poznávací značky (RZ)

– v registru motorových vozidel je vedeno

- značka motorového vozidla
- typ motorového vozidla
- RZ motorového vozidla

- druh motorového vozidla
- barva motorového vozidla
- kategorie motorového vozidla
- majitel a provozovatel motorového vozidla
    - podružně VIN motorového vozidla
    - podružně rok výroby či dovozu či uvedení do provozu motorového vozidla
    - podružně objem a palivo
    - podružně počet míst k sezení, stání, lůžek
    - podružně hmotnost motorového vozidla
    - podružně číslo velkého technického průkazu
    - podružně číslo osvědčení o technickém průkazu
    - podružně seznam technických prohlídek
    - podružně archiv majitelů a provozovatelů vozidla
    - podružně archiv RZ.

4.3.3 Centrální registr zbraní

Informační systém tzv. D-ZBRANĚ je centrální vedený systém ve kterém je vedeno;

- držitel zbraně
- informace o zbrojních průkazech
- informace o zbrojních licencích
- informace o průkazech zbraní
- druh zbraně
- vzor zbraně
- ráže zbraně
- výrobce zbraně
- číslo rámu zbraně
- číslo závěru zbraně
- číslo hlavně zbraně
- rok výroby

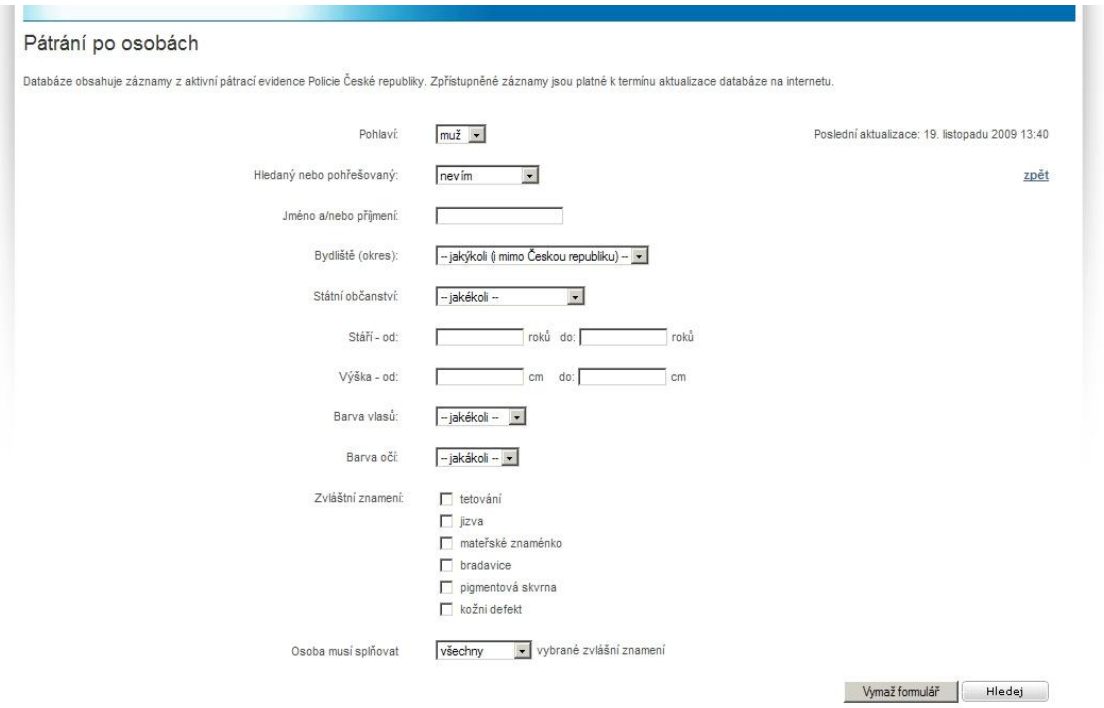
4.3.4 Pátrání po osobách

– evidence pátrání po osobách, je informačním systémem evidence osob, po kterých bylo na území České republiky vyhlášeno pátrání. Jde o osoby pohřešované, hledané, osoby, které nemohou nebo nejsou schopny prokázat svou totožnost, případně nalezené mrtvoly neznámé totožnosti a kosterní nálezy.

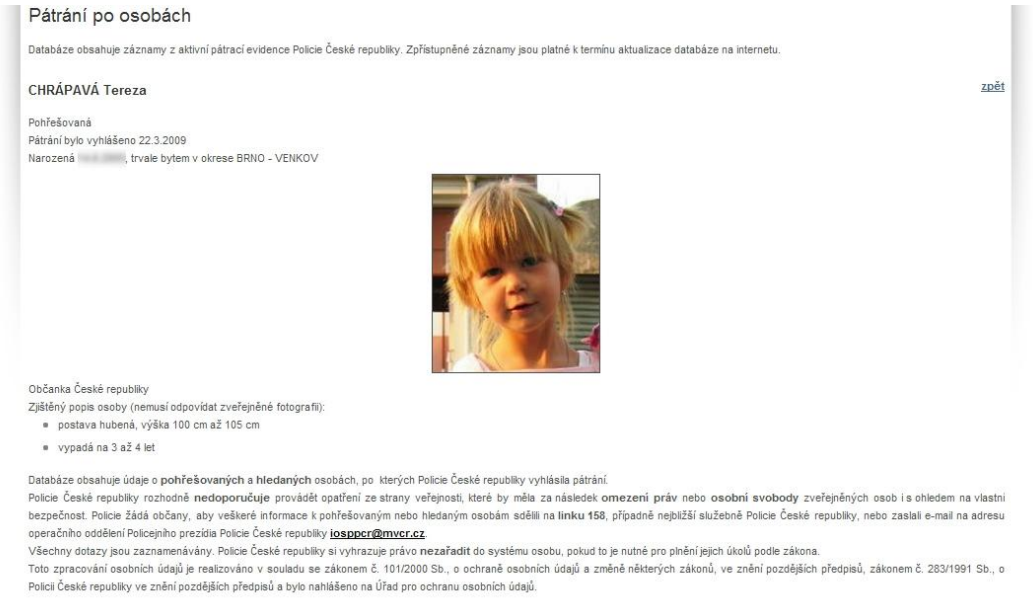
V této evidenci nejsou však vedeny jen osoby, po kterých je pátráno jak v České republice, ale také v Schengenském prostoru z jakéhokoliv důvodu. Tato evidence je v omezeném výstupu deklarována a přístupna veřejnosti a lze se na ní připojit na www internetových stránkách Ministerstva vnitra – Policie ČR. [10] Do datového skladu jsou osoby společně s informacemi vkládány prostřednictvím „ostrého klienta“, kterého mají na svých počítačích nainstalováni specialisti – pátrači v rámci výkonu služby kriminální policie a vyšetřování. Vytěžování však probíhá z online verze jak na intranetových stránkách PČR, tak na internetových stránkách Word Wide Web, kde jsou určené výstupy publikovány.

V této evidenci se vyhledává podle různých kritérií[11], nejčastěji však dle jména, příjmení, data narození či rodného čísla, ale jsou zde možné analytické dotazy se zástupnými znaky „*“ nebo „?“. Zajímavostí je i to, že na internetu se zobrazují fotografie hledaných osob, viz. obrázek č. 7.

[10] Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-19 13:40 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/vozidla/patrani/homepage.php
[11] Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-19 13:41 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/vozidla/patrani/index.php



Obrázek č. 6 – Pátrání po osobách na stránkách MVČR[9]



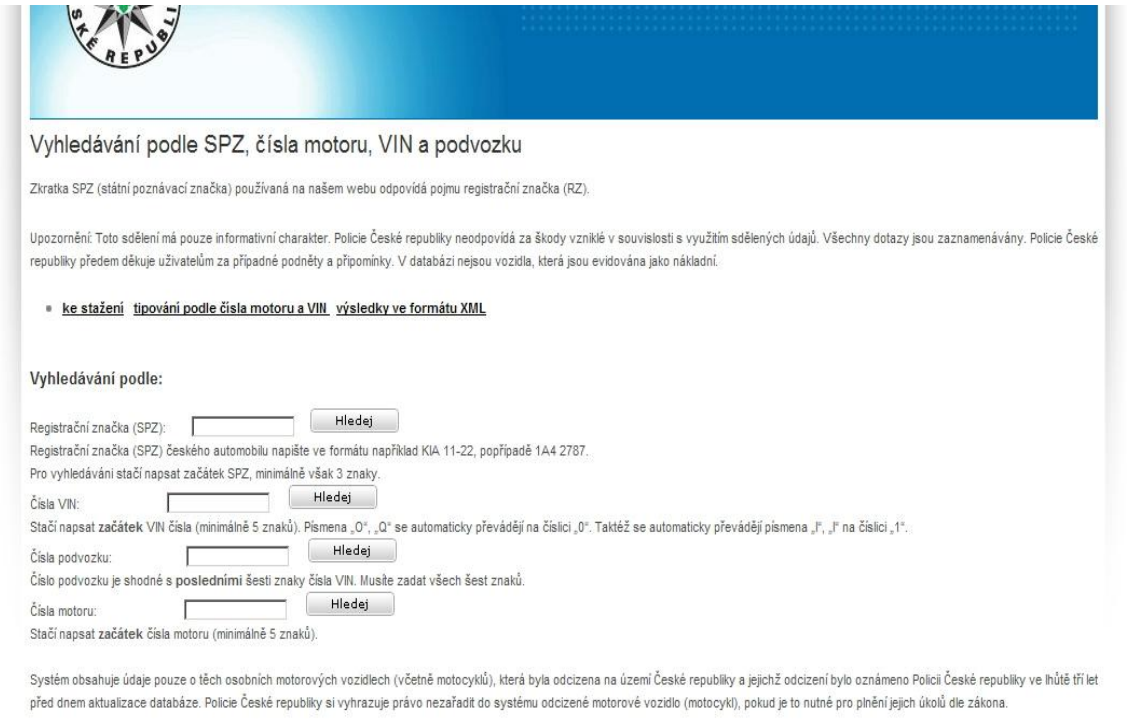
Obrázek č. 7 – list pohřešované osoby[12]

[12] Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-19 13:59 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/vozidla/patrani/detail.php?id=22470322090602

4.3.5 Pátrání po motorových vozidlech

- evidence pátrání po motorových vozidlech

Již s názvem je spjato poslání tohoto informačního systému a to pátrání po odcizených motorových vozidlech, které byly vyhlášeny na území České republiky. Obsahem databáze jsou identifikační údaje vozidla, popis marketů, doba a místo odcizení, informace o majiteli a dále informace k útvaru a případu, který pátrání vyhlásil a zažádal. Dále jsou zde v „archivu“ vedeny údaje o nálezu motorového vozidla ve stejném rozsahu. Při vkládání záznamů v tzv. ostré verzi jsou identifikační údaje osob a vyhlašovaných vozidel přebírány automatizovaným hypertextovým odkazem do ze systému CRO a CRV a tím se snižuje možnost chyb při zápisu. Prostřednictvím Národní ústředny Interpol Praha jsou v systému vedena i vozidla, po kterých pátrají ústředny Interpolu jiných států. Tedy s nadsázkou lze říci, že je jedno, zda se jedná o skútr, čtyřkolku, osobní automobil či autobus, ale tento informační systém stejně jako u pátrání po osobách plní z tzv. „ostrého klienta“ pracovníci – pátrači z oddělení jednotlivých služeben kriminální služby a vyšetřování. Tato „ostrá verze“ je nainstalována také na jednotlivých oprávněných počítačích s hardwarovým klíčem a přes tohoto klienta jsou informace o odcizených motorových vozidlech vkládány. Vytěžování opět je prostřednictvím online informačního systému a je k dispozici na intranetu Policie ČR jako na internetu (Word Wide Webu). Jak již bylo řečeno, jakýkoliv občan může tuto evidenci (informační systém) otevřít na stránkách MVČR – Policie ČR a dotázat se zde, viz. obrázky níže.



Vyhledávání podle SPZ, čísla motoru, VIN a podvozku

Zkratka SPZ (státní poznávací značka) používaná na našem webu odpovídá pojmu registrační značka (RZ).

Upozornění: Toto sdělení má pouze informativní charakter. Policie České republiky neodpovídá za škody vzniklé v souvislosti s využitím sdělených údajů. Všechny dotazy jsou zaznamenávány. Policie České republiky předem děkuje uživatelům za případné podněty a připomínky. V databázi nejsou vozidla, která jsou evidována jako nákladní.

- ke stažení tipování podle čísla motoru a VIN výsledky ve formátu XML

Vyhledávání podle:

Registrační značka (SPZ): Hledej
Registrační značka (SPZ) českého automobilu napište ve formátu například KIA 11-22, popřípadě 1A4 2787.
Pro vyhledávání stačí napsat začátek SPZ, minimálně však 3 znaky.
Čísla VIN: Hledej
Stačí napsat **začátek** VIN čísla (minimálně 5 znaků). Písmena „O", „Q" se automaticky převádějí na číslici „0". Taktéž se automaticky převádějí písmena „I", „I" na číslici „1".
Čísla podvozku: Hledej
Číslo podvozku je shodné s **posledními** šesti znaky čísla VIN. Musíte zadat všech šest znaků.
Čísla motoru: Hledej
Stačí napsat **začátek** čísla motoru (minimálně 5 znaků).

Systém obsahuje údaje pouze o těch osobních motorových vozidlech (včetně motocyklů), která byla odcizena na území České republiky a jejichž odcizení bylo oznámeno Policii České republiky ve lhůtě tří let před dnem aktualizace databáze. Policie České republiky si vyhrazuje právo nezařadit do systému odcizené motorové vozidlo (motocykl), pokud je to nutné pro plnění jejich úkolů dle zákona.

Obrázek č. 8 - dotazový formulář odcizená motorová vozidla[13]

Vyhledávání podle SPZ, čísla motoru, VIN a podvozku

Zkratka SPZ (státní poznávací značka) používaná našem webu odpovídá pojmu registrační značka (RZ).

Upozornění: Toto sdělení má pouze informativní charakter. Policie České republiky neodpovídá za škody vzniklé v souvislosti s využitím sdělených údajů. Všechny dotazy jsou zaznamenávány. Policie České republiky předem děkuje uživatelům za případné podněty a připomínky.

Výsledek vyhledávání podle SPZ:

Poslední aktualizace: 2009-11-19 06:05:00
Dotaz: CBU 48-91*

	SPZ	typ vozu	barva	číslo VIN	číslo motoru
1	**CBU 48-91**	ASIA	červená	KN1CA2125SK022214	78221

Systém obsahuje údaje pouze o těch osobních motorových vozidlech, která byla odcizena na území České republiky a jejichž odcizení bylo oznámeno Policii České republiky ve lhůtě tří let před dnem aktualizace databáze. Policie České republiky si vyhrazuje právo nezařadit do systému odcizené motorové vozidlo, pokud je to nutné pro plnění jejich úkolů dle zákona.

Obrázek č. 9 – výsledek na dotaz pátrání po vozidle[14]

[13] Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-19 14:26 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/auta/index.html

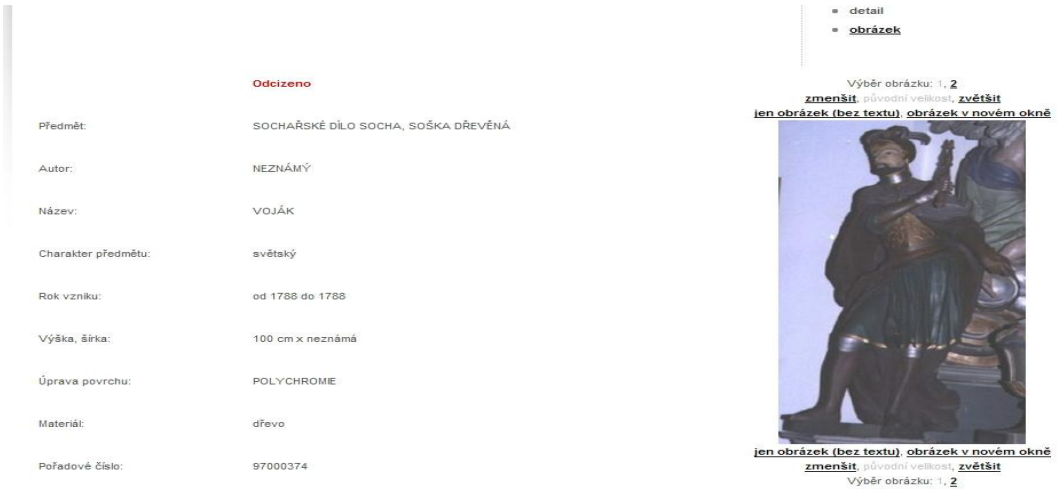
[14] Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-19 14:31 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/vozidla/vozidla/vysledek.php?dotaz=CBU+48-91&akce=vspz

Samozřejmostí zůstává ovšem fakt, že veřejnosti jsou skryty podrobnosti události, pouze získá poznatek, že vozidlo je v pátrání a není s ním vše v pořádku, což může být jako pomůcka při koupi vozidla v autobazaru apod..

4.3.6 Odcizená umělecká díla

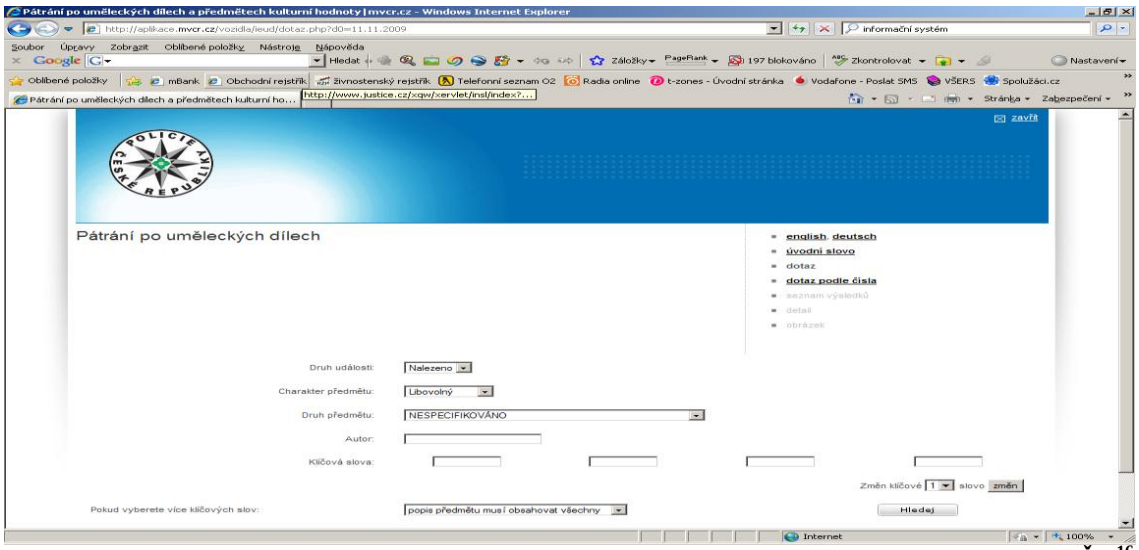
Odcizená umělecká díla jsou evidovány v evidencích Policie ČR pod zkratkou SEUD. SEUD je informační systém, který je plněn pouze od úrovně Krajských ředitelství Policie ČR a výše. Data jsou jednou týdně po zpracování na Úřadu služby kriminální policie a vyšetřování Policejního prezidia přenášena na centrální server, kde je provedena aktualizace centrální databáze. Z této databáze jsou vyexportovány záznamy, položkově zredukované, určené podle zvláštního příznaku ke zveřejnění na internetu a odeslány elektronickou poštou na pracoviště odboru tisku a public relations MV ČR, kde je aktualizována internetová databáze a to nejen v češtině, ale i pro potřeby odborné veřejnosti mutace v anglickém a německém jazyce. Pokud dojde k odcizení např. sochy, která je vyhodnocena jako umělecké dílo, např. v minulosti takto byla řešena krádež soch v rámci Křížové cesty u Římova v okr. České Budějovice. Fotografie jsou umístěny s detailním popisem do tohoto informačního systému, který je možno vytěžovat buď přímo aplikačním rozcestím SEUD nebo IS Policie. Každý předmět dostává své deseti místné ID číslo, které je nezaměnitelné a pod kterým je předmět vyhlášen k pátrání. Stejně jako pátrání po osobách a pátrání po motorových vozidlech, má každý občan možnost nahlédnout z Word Wide Web na vyhledávací formulář SEUD na stránkách MVČR – Policie ČR a dotyčný předmět dohledat. Jako dokládací tohoto přikládám již zmíněnou sochu vojáka, který byl odcizen z katastru obce Římov v tomto roce[15]. Bohužel tímto se odstartovala vlna krádeží těchto soch a v této době již v Římově a okolí nenajdeme ani jednu sochu, jelikož to, co nestačili pachatelé odcizit, státní úředníci zbylé sochy uschovali do depozitářů v Českých Budějovicích.

[15] Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-19 14:47 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/vozidla/ieud/detail.php?pc=97000374&du=O&cp=s&kp=C&k1=VOJÁK&mx=21&de=3&d0=11.11.2009



Obrázek č. 10 – výsledek na dotaz SEUD na stránkách MVČR[13]

V tomto informačním systému však nejsou vedeny nejen odcizené předměty, ale velkou část databáze tvoří nalezené předměty, u kterých se pátrá po jejich původu. Systém je veden od roku 2000.



Obrázek č. 11 – výsledek na dotaz SEUD na stránkách MVČR[16]

4.3.7 Databáze pátrání po původu a majiteli předmětů

Tato databáze je pouze internetová a je zveřejněna na Word Wide Webu na stránkách Ministerstva vnitra v záložce „Databáze“[17]. Slouží široké veřejnosti, aby

[16] Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-20 19:51 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/vozidla/ieud/dotaz.php?d0=11.11.2009

identifikovala vystavené předměty, které byly policií nalezeny nebo zajištěny například při domovních prohlídkách nebo prohlídkách jiných prostor a do této doby policisté neznají majitele nebo již zmíněný původ oné věci. Většinou se zde vystavují pouze věci vyšší hodnoty, starožitnosti nebo věci, které mají jinou, ale určitou hodnotu. Tato databáze je aktualizována policisty kriminální služby a vyšetřování Policejního prezidia, odboru pátrání, kam určité žádosti zasílají jednotlivé územní odbory jednotlivých krajských ředitelství policie. Tedy dalo by se říci, že tato databáze není informačním systémem Policie ČR, ale službou Policie ČR veřejnosti, nicméně policie má taxativně dané povinnosti dle § 2 zákona o Policii ČR a proto se jedná i o velmi důležitý informační systém v rámci rodiny informačních systémů u ministerstva vnitra a policie jako takové.

Obrázek č. 12 – pátrání po původu a majiteli předmětů[18]

4.3.8 Kriminalistický ústav a informační databáze (sbírky)

Kriminalistický ústav s hlavním sídlem v Praze vede národní sbírky, které jsou vedeny centrálně a sdružuje například nejznámější sbírku Národní databáze DNA. Tyto sbírky můžeme nazývat specializovanými, laboratorními a expertními informačními

[17] Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-20 19:58 hod.). Dostupný z WWW http://www.policie.cz/clanek/patrani-po-majiteli-predmetu-patrani-po-puvodu-a-majiteli-predmetu.aspx

[18] Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-20 20:12 hod.). Dostupný z WWW: http://www.policie.cz/clanek/patrani-po-majiteli-predmetu-patrani-po-puvodu-a-majiteli-predmetu.aspx

systémy. Tyto slouží ke specifické činnosti a mají zpravidla identifikační, analytický a vědeckotechnický charakter. V této skupině nalézáme informační technologie pro zpracování a analýzu obrazových, textových, zvukových a dalších informací, pro identifikaci na základě otisků prstů, DNA, hlasu, portrétu osoby. *Řadí se sem elektronické systémy biologické i chemické analýzy, systémy na podporu zpracování poznatků z trasologie, mechanoskopie apod.. Tyto informační systémy podporují matematické, fyzikálně – technické modelování, soudní lékařství a inženýrství, analýzu dopravních nehod apod..* [19]

Mezi jednotlivé výše uvedené systémy bychom mohli zařadit mnoho systémů, které nezúčastněné osobě nic neřeknou, nicméně v souvislostech věci je zde vhodné se o nich alespoň zmínit. Je zde vedena již zmiňovaná národní databáze DNA, dále databáze TRASIS – trasologický identifikační systém, USBS – ústřední sbírka balistických stop, IDENTOS – sbírka deportovaných lebek a kosterních nálezů. Ale také SQUAMOS – sbírka rybích šupin a nebo PENAEOS – sbírka ptačích per.

5 OPERAČNÍ PROSTOR A TAXATIVNĚ VYMEZENÉ ÚKOLY POLICIE ČESKÉ REPUBLIKY / exkurs k vybraným ustanovením zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů /

5.1 Operační prostor a základní vymezení

Policie České republiky má taxativně vymezené úkoly, které má plnit a to v zákoně číslo 273/2008 Sb. O Policii České republiky, kde v § 2 je uvedeno;

„*Policie slouží veřejnosti. Jejím úkolem je chránit bezpečnost osob a majetku 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*

[19] Jiří Štraus a kolektiv, Kriminalistická technika, 2. rozšířené vydání, Aleš Čeněk, s.r.o., Praha 2008, ISBN 978-80-7380-095-6

Evropských společenství nebo mezinárodními smlouvami, které jsou součástí právního řádu“[20]

5.2 Taxativní vymezení

5.2.1 chránit bezpečnost osob a majetku

Se spojením informačních systémů lze s určitostí říci, že jde o úzké propojení těchto dvou, při prvním pohledu, vzdálených věcí. Když si uvědomíme, tak v dnešní době skoro všechno vychází z výpočetní techniky a s tím spojených věcí. Chránit bezpečnost je povinností policie daná normou a policie k tomuto využívá informační technologie a informační systémy od prvopočátku věci. Jako příklad by šlo uvést, informační systém Centrum dopravních informací. V tomto jsou z celé republiky evidovány, vkládány a vytěžovány dopravní informace a to nejen o dopravních nehodách, ale i o uzavírkách, kolonách, sjízdnosti silnic, stav na hraničních přechodech, kamerové záznamy z dálnic, měst apod. Nejde jen o policejní systém, ale policie ho jistě využívá k předcházení stavů, které by ohrožovaly bezpečnost osob a majetku. Navíc Policie distribuuje tyto informace sdělovacím prostředkům a tyto určité události šíří dál[21] tak, aby se dostaly k co nejvíce lidem. Dalším příkladem, kdy policie chrání bezpečnost osob a majetků jsou kamerové záznamy např. z městských kamerových systémů, které jsou shromažďovány po dobu několika měsíců v datových skladech a na operačních střediscích Policie ČR či městské policie slouží k předcházení páchání trestné činnosti, předcházení dopravních komplikací či životů samotných. Z praxe lze uvést příklad, kdy osobu napadla skupinka 4 osob, tohoto všichni zúčastnění kopali a dokonce i chtěli použít nůž k pobodání poškozeného, nicméně díky kamerovému systému o tomto operační středisko již vědělo a na místo vyslalo hlídky a tyto v poslední chvíli předešly možná smrtelnému napadení poškozeného – tedy je zde i symbolizováno motto policie – Pomáhat a chránit.

[20] Škoda J., Vavera F., Šmerda R., Zákon o policii s komentářem, Aleš Čeněk, s.r.o., Praha 2009, 34 s, ISBN 978-80-7380-160-1

[21] Škoda J., Vavera F., Šmerda R., Zákon o policii s komentářem, Aleš Čeněk, s.r.o., Praha 2009, 35 s, ISBN 978-80-7380-160-1

5.2.2 Předcházet trestné činnosti

Je další taxativně danou povinností policie, přičemž i k tomuto a hlavně k tomuto slouží mnoho již zmíněných i nezmíněných informačních systémů. Informační systém kriminalistické sledované události slouží například policii k evidenci trestných činů, které se v minulosti staly, nicméně je známé to, že jen málokterý pachatel se dopustí stejného činu jen jednou, většinou se v trestné činnosti opakuje a není dogma, že by se tak mělo stávat jen na jednom místě, např. v okrese Písek. Díky těmto informačním systémům, mezi nimiž je i již zmiňovaný „Kriminalistické sledované události" je policista, a je jedno, zda se jedná o policistu zařazeného na obvodním oddělení, nebo na službě kriminální policie a vyšetřování nebo na kterémkoliv služebním místě, schopen ze sestav informačních systémů zjistit podobnost určité trestné činnosti a když ne přesně definovat určitého pachatele, tak výrazně napomoci k jeho zjištění a ustanovení jeho totožnosti. Když uvádím různé sestavy, v určitých informačních systémech lze docílit sestav dle popisu osob, což se využívá hlavně k předcházení násilné, mravnostní či jiné trestné činnosti, kde poškozený nebo svědek vidí pachatele a dokáže tohoto popsat nebo u těch činů, kde již pachatel je policii již znám a policista učiní jeho laický popis a zapíše jej do datového skladu určitého informačního systému. Dále jsou sestavy, jimiž se určují pachatelé dle způsobu provedení trestné činnosti. Zde se jedná hlavně o krádeže (dle § 205 zák. číslo 40/2009 Sb.), krádeže vloupáním (dle § 205/b zák. číslo 40/2009 Sb.), poškozování cizí věci (dle § 228 zák. číslo 40/2009 Sb.) či loupeže (dle § 173 zák. č. 40/2009 Sb.). Každý pachatel má totiž na místě individuální jednání a na místě nezanechává jen biologické, daktyloskopické, chemické, pachové, v některých případech i balistické, ale i stopy mechanoskopické, mikro stopy či věcné stopy. Mechanoskopické stopy nám vypovídají velmi často o např. způsobu vniknutí a porušení zámků FAB, kdy policie zjistí, zda byl zámek páčen, vrtán, zda byl odemčen shodným klíčem a dokáže i dokonce přesně určit předmět, kterým byl zámek poškozen. Samozřejmě, že toto se zadává do speciálních informačních systémů a je zde možno tzv. „natipovat" pachatele a tím předejít páchání jeho další trestné činnosti. Nicméně sestavy nejsou tvořeny vždy odborným zkoumáním, ale někdy může stačit znát tu skutečnost, že pachatel nosí sekyru, kterou rozseká na určitých místech dveře či okna a vniká tímto způsobem do rekreačních chat. V době, kdy se k této informaci přidá ještě např. určitá denní či noční doba, místo a

třeba i zajištěná jiná stopa, lze pachatele ustanovit a sestavou „k tomuto najít cestu“. Policista i v tomto případě předchází páchání trestné činnosti a tím chrání bezpečnost osob a majetku.

5.2.3 Oprávnění dle § 66 zákona č. 273/2008 Sb., o Policii ČR, ve znění pozdějších předpisů

Dalším úkolem je plnit úkoly podle trestního řádu a další úkoly na úseku vnitřního pořádku a bezpečnosti svěřené jí zákony. K tomuto využívá oprávnění policie například s využitím § 66 zákona č. 273/2008 Sb. o Policii České republiky, ve znění pozdějších předpisů, který hovoří o získávání informací z evidencí takto;

- *§ 66 odst. 1 cit. zákona č. 273/2008 Sb. - Policie může v rozsahu potřebném pro plnění konkrétního úkolu žádat od správce evidence nebo zpracovatele poskytnutí informací z evidence provozované na základě jiného právního předpisu. Správce evidence nebo zpracovatel poskytne informace bezplatně, nestanoví-li jiný právní předpis jinak. Správce evidence nebo zpracovatel jsou povinni žádosti bez zbytečného odkladu vyhovět, nestanoví-li jiný právní předpis pro poskytnutí informací policii jiný režim.*

- *§ 66 odst. 2 cit. zákona č. 273/2008 Sb. - Policie může v rozsahu potřebném pro plnění konkrétního úkolu žádat od správce evidence nebo zpracovatele poskytnutí informací z databáze účastníků veřejně dostupné telefonní služby, evidence občanských průkazů, evidence cestovních dokladů, evidence diplomatických a služebních pasů, informačního systému evidence obyvatel, evidence motorových vozidel, registru rodných čísel, evidence údajů o mýtném, katastru nemovitosti a registru řidičů způsobem umožňujícím dálkový a nepřetržitý přístup; v případě evidence občanských průkazů a evidence cestovních dokladů lze informace poskytnout způsobem umožňujícím pouze nepřetržitý přístup; v případě databáze účastníků veřejně dostupné telefonní služby se informace poskytne ve formě a v rozsahu stanoveném jiným právním předpisem.*

- *§ 66 odst. 3 cit. zákona č. 273/2008 Sb. - Policie může v případech stanovených zákonem a v rozsahu potřebném pro plnění konkrétního úkolu žádat od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací poskytnutí provozních a lokalizačních údajů způsobem umožňujícím dálkový a nepřetržitý přístup, nestanoví-li jiný právní předpis jinak. Tyto osoby jsou povinny žádosti vyhovět bez zbytečného odkladu, ve formě a v rozsahu stanoveném jiným právním předpisem.*

- *§ 66 odst. 4 cit. zákona č. 273/2008 Sb. - Policie žádá o poskytnutí informací podle odstavců 1 až 3 pouze způsobem, který umožní policii uchovávat identifikační údaje o útvaru policie nebo o policistovi, který o poskytnutí informací žádal, a o účelu, k němuž bylo o poskytnutí informací žádáno, nejméně po dobu 5 let. O skutečnostech podle věty první jsou správce evidence nebo zpracovatel povinni zachovávat mlčenlivost.*

- *§ 66 odst. 5 cit. zákona č. 273/2008 Sb. - Za účelem zajištění ochrany osoby, o níž lze důvodně předpokládat, že by mohl být ohrožen její život nebo zdraví, nebo pro účely pátrání po hledané anebo pohřešované osobě mohou policie nebo ministerstvo požadovat od zpracovatele nebo správce evidence vedené na základě jiných právních předpisů, aby policii oznamovali každý výdej osobních údajů.*[22]

Tyto ustanovení se využívají v mnoha případech a jsou to jak vstupy do analytických informačních systémů, tak výstupy z běžných tak analytických informačních systémů. Případem, kdy tento postup může být uplatněn je například výpis IMEI dle telefonního čísla určitého mobilního operátora. V případě, že znám telefonní číslo mobilního operátora, zadám prostřednictvím informačního systému požadavek na specializované pracoviště Policie ČR k dohledání, toto specializované pracoviště v součinnosti s mobilním operátorem z jiného informačního systému udělá výstup, z jakých mobilních telefonů (IMEI) bylo za určité období voláno a toto opět informačním

[22] Škoda J., Vavera F., Šmerda R., Zákon o policii s komentářem, Aleš Čeněk, s.r.o., Praha 2009, 316 - 225 s, ISBN 978-80-7380-160-1

systémem, prvotním zadáním odešle vyžadujícímu policistovi, který si tento výsledek vyzvedne. Poté s výstupem a zjištěným materiálem může dále pracovat v dalších, již v této bakalářské práci neuvedených informačních systémech v analytické úrovni. Tedy policie plní další taxativně danou povinnost.

5.2.4 Využití § 16 zákona č. 273/2008 Sb., o Policii ČR, ve znění pozdějších předpisů

Dalším bodem využití informačních systémů spojených s policií či dokonce zákonem č. 283/2008 Sb. o Policii ČR, ve znění pozdějších předpisů je mimo jiné § 16 tohoto zákona hovořící o;

- *odst. 1; Útvar policie určený policejním prezidentem může uzavřít písemnou koordinační dohodu s obcí nebo městskou částí hlavního města Prahy za účelem stanovení společného postupu při zabezpečování místních záležitostí veřejného pořádku.*
- *odst. 2; Místně příslušné krajské ředitelství může uzavřít písemnou koordinační dohodu s hlavním městem Prahou za účelem stanovení společného postupu při zabezpečování místních záležitostí veřejného pořádku.*
- *odst. 3; Koordinační dohoda obsahuje zejména*
    - *písm. a) formy a nástroje nepřetržité koordinace obce a útvaru policie při zabezpečování místních záležitostí veřejného pořádku v obci,*
    - *písm. b) úkoly obce a útvaru policie v oblasti předcházení protiprávním jednáním porušujícím veřejný pořádek v obci,*
    - *písm. c) úkoly obce a útvaru policie při porušení veřejného pořádku v obci,*
    - *písm. d) podíl obce a útvaru policie na zajištění plnění úkolů podle písmen b) a c),*
    - *písm. e) formy a nástroje hodnocení plnění úkolů podle písmen b) a c) a odstraňování případných zjištěných nedostatků,*
    - *písm. f) dobu, na kterou je uzavírána,*

- *písm. g) poskytování finančních prostředků*[23]

Pokud je přečten text z odstavce 1 výše uvedeného § 16 zákona o Policii ČR je jasné, že o tomto již bylo v této bakalářské práci psáno. Jedná se o podpis určitých dokumentů, například o využívání městského kamerového systému jak městskou policií, potažmo městem samotným, tak Policií ČR a to ať na online verzi či offline verzi. A nejsou to jenom kamerové záznamy, ale i v blízké minulosti zavedené parkovné, které je placeno mobilním telefonem nebo prostřednictvím internetu (Word Wide Web). K tomuto následně slouží také informační systém, který mají v online verzi jak městští strážníci, tak policisté dopravní policie ČR a jsou díky tomuto systému schopni určit, zda jde v tomto případě o přestupkové jednání občana, nebo zda je vše v pořádku.

„Dne 20. srpna 2009 byla primátorem statutárního města České Budějovice Jurajem Thomou a plukovník Ladislavem Škvařilem podepsána koordinační dohodu o spolupráci mezi městem a Policií ČR. Dohoda vymezuje kompetence města (resp. městské policie) a Policie ČR při zajišťování veřejného pořádku a bezpečnosti na území města. „Je to vůbec poprvé, kdy taková dohoda vznikla. Dohoda je formálním završením dosavadní úzké spolupráce mezi městem a Policií ČR, která se datuje od začátku současného volebního období," upozornil primátor. Od roku 2006 totiž zve primátor Thoma zástupce Policie ČR na každoměsíční schůzky, na nichž se projednává společný postup městské a státní policie nejen při mimořádných akcích, ale i při běžné hlídkové činnosti. Spolupráce funguje nejen na nejvyšší úrovni vedení, ale i na úrovni operačních středisek městské policie a Policie ČR a také přímo v hlídkové službě v rámci obvodů. „Díky vzájemné koordinaci se hlídková činnost městské a státní policie zbytečně nepřekrývá. Kriminalita na územích Českých Budějovic tak v poslední době setrvale klesá."."[24]

[23] Zákon číslo 273/2008 Sb. o Policii ČR , publikace „Zákon o policii s komentářem", Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., Praha 2009, 67 – 69 s, ISBN 978-80-7380-160-1

[24] Dokument DOHODA O VZÁJEMNÉ SPOLUPRÁCIPŘI ZABEZPEČOVÁNÍ MÍSTNÍCH ZÁLEŽITOSTÍ VEŘEJNÉHO POŘÁDKU vydaná Magistrátem města české Budějovice 09/2009, Oficiální stránky Magistrátu statutárního města České Budějovice (online) 2010 (cit. 2010-02-15 20:27 hod.). Dostupný z WWW: http://www.c-budejovice.cz/cz/mesto/aktuality/Documents/09-08-20_Koordinační%20dohoda%20s%20PČR.pdf

5.3 Oprávnění dle zákona č. 306/2009 Sb., o Policii ČR, ve znění pozdějších předpisů

Policie České republiky má vymezené možnosti k využití různých ustanovení uvedených např. v zákoně č. 306/2009 Sb., o trestním řízení soudním, kterým se s platností od 4. 9. 2009 a účinností od 1. 1. 2010 mění zákon č. 40/2009 trestní zákoník a další zákony.

V hlavě IV. tohoto zákona je uvedena i změna trestního řádu (zákona č. 141/1961, Sb., ve znění pozdějších předpisů), kdy v oddílu čtvrtém v §§ 83, 83a cit. zákona je mimo jiné taxativně uvedeno;

- *§ 83 cit. zákona č. 141/1961 Sb. - Příkaz k domovní prohlídce*
  - *odst. 1 - Nařídit domovní prohlídku je oprávněn předseda senátu a v přípravném řízení na návrh státního zástupce soudce. V neodkladných případech tak může namísto příslušného předsedy senátu nebo soudce (§ 18) učinit předseda senátu nebo soudce, v jehož obvodu má být prohlídka vykonána. Příkaz k domovní prohlídce musí být vydán písemně a musí být odůvodněn. Doručí se osobě, u níž se prohlídka koná, při prohlídce, a není-li to možné, nejpozději do 24 hodin po odpadnutí překážky, která brání doručení.*
  - *odst. 2 - Na příkaz předsedy senátu nebo soudce vykoná domovní prohlídku policejní orgán.*
- *§ 83a cit. zákona č. 141/1961 Sb. - Příkaz k prohlídce jiných prostor a pozemků*
  - *odst. 1 - Nařídit prohlídku jiných prostor nebo pozemků je oprávněn předseda senátu, v přípravném řízení státní zástupce nebo policejní orgán. Policejní orgán k tomu potřebuje předchozí souhlas státního zástupce. Příkaz musí být vydán písemně a musí být odůvodněn. Doručí se uživateli dotčených prostor nebo pozemků, a nebyl-li zastižen při prohlídce, bezprostředně po odpadnutí překážky, která doručení brání.*
  - *odst. 2 - Prohlídku jiných prostor nebo pozemků provede orgán, který ji nařídil, nebo na jeho příkaz policejní orgán.*

- *odst. 3 - Bez příkazu nebo souhlasu uvedeného v odstavci 1 může policejní orgán provést prohlídku jiných prostor nebo pozemků jen tehdy, jestliže příkazu nebo souhlasu nelze předem dosáhnout a věc nesnese odkladu, nebo v případě, že uživatel dotčených prostor nebo pozemků písemně prohlásí, že s prohlídkou souhlasí, a své prohlášení předá policejnímu orgánu. O tomto úkonu však musí bezprostředně uvědomit orgán, který je k vydání příkazu nebo souhlasu uvedenému v odstavci 1 oprávněn.*[25]

I ve výše uvedených oprávněních figurují informační systémy od prvopočátku až k samotné domovní prohlídce. Vlastní postup získávání povolení domovní prohlídky bytových či nebytových prostor, policejní orgán musí dokladovat ve spisovém materiálu jak majitele pozemků, budov či automobilů a jiných prostor tím, že využívá dálkového přístupu do informačního systému „Katastr“, který je zpřístupněný bezúplatně prostřednictvím Policejního prezidia ČR z datových skladů Katastrálního a zeměměřičského úřadu České republiky. Nejde tedy o informační systém provozovaný policií, ale policie velmi často a efektivně využívá výstupy z tohoto systému. V tomto se dají nalézt informace např. dle rodných čísel občanů, listů vlastnictví kdekoliv v katastrálním území v České republice či dle čísel budov nebo pozemků. Tento systém de-facto kopíruje veřejně přístupný portál Katastrálního a zeměměřičského úřadu[26], kde lze nalézt totožné informace, byť s menšími možnostmi vyhledávání, ale v zásadním a neopomenutelném rozdílu. Tento rozdíl je v tom, že výstup z dálkového přístupu do katastru nemovitostí je oficiálním dokumentem, který je platný 3 měsíce a lze využít jako podklad soudci či státnímu zástupci, který následně rozhoduje o vydání či zamítnutí žádosti Policie ČR o vydání příkazu k domovní prohlídce či prohlídce jiných prostor a pozemků. V době, kdy již má policista vydán uvedený příkaz a domovní prohlídku vykonává na místě, na analytickém pracovišti policista prostřednictvím radiokomunikačního přístroje provádí lustraci nalezených věcí. Velmi často se stává, že věci z domovních prohlídek pocházejí z trestné činnosti a jejich popis a hlavně výrobní čísla jsou vodítkem k případům či poškozeným, kterým tímto odcizením vznikla škoda.

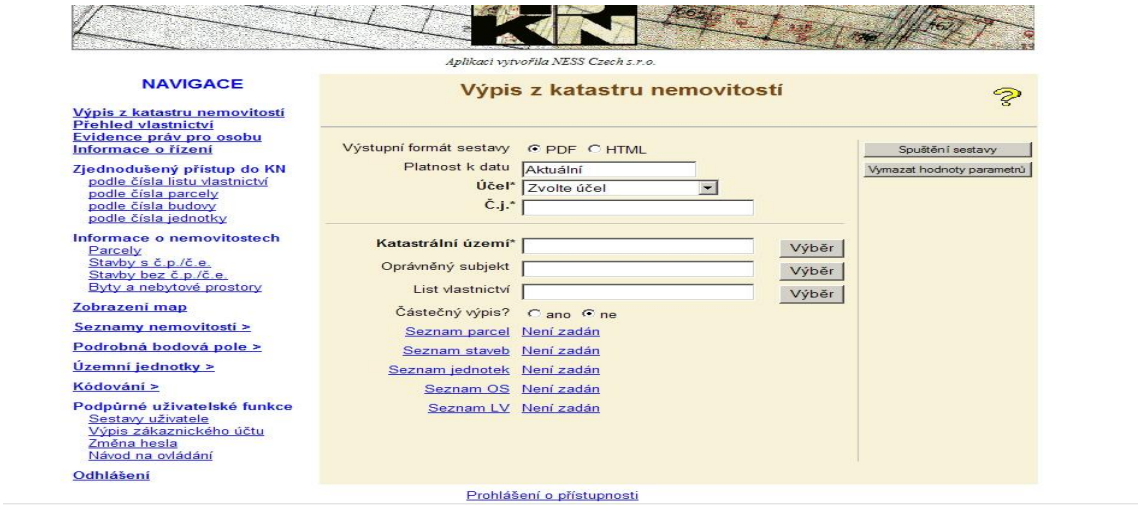
[25] Jelínek J. a kol., Trestní zákoník a trestní řád s poznámkami a judikaturou, 1. vydání, Praha: Leges, 2009, 235 s, ISBN: 978-80-87212-22-6

[26] Oficiální stránky Katastrálního a zeměměřičského úřadu – Katastr nemovitostí ČR (online) 2009 (cit. 2009-11-23 03:02 hod.). Dostupný z WWW: http://nahlizenidokn.cuzk.cz/

Tedy, zde se setkává opět policejní úkon s informační technologií. K tomuto účelu je určený již zmíněný informační systém Kriminalisticky sledované události, kde se zaznamenává nejen výrobní číslo, ale např. značka, barva, popis věci. Dále je využíván pátrací systém po odcizených vozidlech, registračních značkách – IS Pátrání po motorových vozidlech. Samozřejmě, že po ukončení domovní prohlídky se zjištěné okolnosti zapisují do dalších informačních systémů, které však nelze jmenovat.

Obrázek č. 13 – Vstupní formulář IS Katastr[27]

[27] Oficiální stránky Katastrálního a zeměměřičského úřadu – Katastr nemovitostí ČR (online) 2009 (cit. 2009-11-22 23:52 hod.). Dostupný z WWW: https://katastr.cuzk.cz/uvod/?enc=windows-1250



Obrázek č. 14 – vyhledávací formulář IS Katastr[28]

Dalším využitím výše uvedeného zákona ve spojitosti s informačními technologiemi je § 88, kde je uvedeno;

Odposlech a záznam telekomunikačního provozu

- *§ 88 cit. zákona č. 141/1961 Sb.*
  - *odst. 1 - Je-li vedeno trestní řízení pro zvlášť závažný zločin nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, může být vydán příkaz k odposlechu a záznamu telekomunikačního provozu, pokud lze důvodně předpokládat, že jím budou získány významné skutečnosti pro trestní řízení a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené. Odposlech a záznam telekomunikačního provozu provádí pro potřeby všech orgánů činných v trestním řízení Policie České republiky. Provádění odposlechu a záznamu telekomunikačního provozu mezi obhájcem a obviněným je nepřípustné. Zjistí-li policejní orgán při odposlechu a záznamu telekomunikačního provozu, že obviněný komunikuje se svým obhájcem, je povinen záznam odposlechu bezodkladně zničit a informace, které se v této souvislosti dozvěděl, nijak nepoužít. Protokol o zničení záznamu založí do spisu.*

[28] Oficiální stránky Katastrálního a zeměměřičského úřadu – Katastr nemovitostí ČR (online) 2009 (cit. 2009-11-23 00:24 hod.). Dostupný z WWW: https://katastr.cuzk.cz/rdp/ActionLogIn.do?PAR_LoggedSessionID=0afc666530d642bae9404a954127a900ba96e2bf9a9e&enc=windows-1250

- *odst. 2 - Nařídit odposlech a záznam telekomunikačního provozu je oprávněn předseda senátu a v přípravném řízení na návrh státního zástupce soudce. Příkaz k odposlechu a záznamu telekomunikačního provozu musí být vydán písemně a musí být odůvodněn, včetně konkrétního odkazu na vyhlášenou mezinárodní smlouvu v případě, že se vede trestní řízení pro úmyslný trestný čin, k jehož stíhání tato mezinárodní smlouva zavazuje. V příkazu k odposlechu a záznamu telekomunikačního provozu musí být stanovena uživatelská adresa či zařízení a osoba uživatele, pokud je její totožnost známa, a doba, po kterou bude odposlech a záznam telekomunikačního provozu prováděn, která nesmí být delší než čtyři měsíce; v odůvodnění musí být uvedeny konkrétní skutkové okolnosti, které vydání tohoto příkazu, včetně doby jeho trvání, odůvodňují. Příkaz k odposlechu a záznamu telekomunikačního provozu se bezodkladně doručí policejnímu orgánu. V přípravném řízení opis příkazu k odposlechu a záznamu telekomunikačního provozu soudce bezodkladně zašle státnímu zástupci.*
- *odst. 3 - Policejní orgán je povinen průběžně vyhodnocovat, zda i nadále trvají důvody, které vedly k vydání příkazu k odposlechu a záznamu telekomunikačního provozu. Pokud důvody pominuly, je povinen odposlech a záznam telekomunikačního provozu ihned ukončit, a to i před skončením doby uvedené v odstavci 2. Tuto skutečnost bezodkladně písemně oznámí předsedovi senátu, který příkaz k odposlechu a záznamu telekomunikačního provozu vydal, a v přípravném řízení rovněž státnímu zástupci a soudci.*
- *odst. 4 - Na základě vyhodnocení dosavadního průběhu odposlechu a záznamu telekomunikačního provozu může soudce soudu vyššího stupně a v přípravném řízení na návrh státního zástupce soudce krajského soudu dobu trvání odposlechu a záznamu telekomunikačního provozu prodloužit, a to i opakovaně, vždy na dobu nejdéle čtyř měsíců.*
- *odst. 5 - Bez příkazu k odposlechu a záznamu telekomunikačního provozu může orgán činný v trestním řízení nařídit odposlech a záznam telekomunikačního provozu, nebo jej provést i sám, je-li vedeno trestní řízení pro trestný čin obchodování s lidmi (§ 168 trestního zákoníku),*

svěření dítěte do moci jiného (§ 169 trestního zákoníku), omezování osobní svobody (§ 171 trestního zákoníku), vydírání (§ 175 trestního zákoníku), únosu dítěte a osoby stižené duševní poruchou (§ 200 trestního zákoníku), násilí proti skupině obyvatelů a proti jednotlivci (§ 352 trestního zákoníku) nebo nebezpečného vyhrožování (§ 353 trestního zákoníku), pokud s tím uživatel odposlouchávané stanice souhlasí.

- odst. 6 - *Má-li být záznam telekomunikačního provozu užit jako důkaz, je třeba k němu připojit protokol s uvedením údajů o místě, času, způsobu a obsahu provedeného záznamu, jakož i o orgánu, který záznam pořídil. Ostatní záznamy je povinen policejní orgán označit, spolehlivě uschovat tak, aby byla zajištěna ochrana před neoprávněným zneužitím záznamů, a v protokolu založeném do spisu poznamenat, kde jsou uloženy. V jiné trestní věci, než je ta, v níž byl odposlech a záznam telekomunikačního provozu proveden, lze záznam jako důkaz užít tehdy, pokud je i v této věci vedeno trestní stíhání pro trestný čin uvedený v odstavci 1, nebo souhlasí- li s tím uživatel odposlouchávané stanice.*
- odst. 7 - *Pokud při odposlechu a záznamu telekomunikačního provozu nebyly zjištěny skutečnosti významné pro trestní řízení, je policejní orgán po souhlasu soudu a v přípravném řízení státního zástupce povinen záznamy bezodkladně zničit po třech letech od pravomocného skončení věci. Byl-li policejní orgán vyrozuměn o podání mimořádného opravného prostředku v uvedené lhůtě, zničí záznamy o odposlechu po rozhodnutí o mimořádném opravném prostředku, případně až po novém pravomocném skončení věci. Protokol o zničení záznamu o odposlechu zašle policejní orgán státnímu zástupci, jehož rozhodnutím byla věc pravomocně skončena, a v řízení před soudem předsedovi senátu prvého stupně, k založení do spisu.*
- odst. 8 - *Státní zástupce, jehož rozhodnutím byla věc pravomocně skončena, a v řízení před soudem předseda senátu soudu prvého stupně po pravomocném skončení věci, informuje o nařízeném odposlechu a záznamu telekomunikačního provozu osobu uvedenou v odstavci 2, pokud je známa. Informace obsahuje označení soudu, který vydal příkaz k odposlechu a záznamu telekomunikačního provozu, délku trvání*

odposlechu a datum jeho ukončení. Součástí informace je poučení o právu podat ve lhůtě šesti měsíců ode dne doručení této informace Nejvyššímu soudu návrh na přezkoumání zákonnosti příkazu k odposlechu a záznamu telekomunikačního provozu. Informaci podá předseda senátu soudu prvého stupně bezodkladně po pravomocném skončení věci; státní zástupce, jehož rozhodnutím byla věc pravomocně skončena, podá informaci bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí nejvyšším státním zástupcem podle § 174a.

- *odst. 9 - Informaci podle odstavce 8 předseda senátu nebo státní zástupce nepodá v řízení o zvlášť závažném zločinu spáchaném organizovanou skupinou, v řízení o trestném činu spáchaném ve prospěch organizované zločinecké skupiny, v řízení o trestném činu účasti na organizované zločinecké skupině (§ 361 trestního zákoníku), nebo pokud se na spáchání trestného činu podílelo více osob a ve vztahu alespoň k jedné z nich nebylo trestní řízení doposud pravomocně skončeno, nebo pokud je proti osobě, jíž má být informace sdělena, vedeno trestní řízení, anebo pokud by poskytnutím takové informace mohl být zmařen účel trestního řízení, včetně řízení uvedeného v odstavci 6, nebo by mohlo dojít k ohrožení bezpečnosti státu, života, zdraví, práv a svobod osob.*

- *§ 88a cit. zákona č. 141/1961 Sb.*
  - *odst. 1 - Je-li k objasnění skutečností důležitých pro trestní řízení třeba zjistit údaje o uskutečněném telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, nařídí předseda senátu a v přípravném řízení soudce, aby je právnické nebo fyzické osoby, které vykonávají telekomunikační činnost, sdělily jemu a v přípravném řízení buď státnímu zástupci nebo policejnímu orgánu. Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn.*

- *odst. 2 - Příkazu podle odstavce 1 není třeba, pokud k poskytnutí údajů dá souhlas uživatel telekomunikačního zařízení, ke kterému se mají údaje o uskutečněném telekomunikačním provozu vztahovat.*[29]

I v těchto ustanoveních se setkává informační technologie s policejní „rutinou". Dle výše uvedených paragrafů se zkráceně řečeno vyžaduje jak aktivní, tak pasivní telekomunikační provoz a to buď se souhlasem majitele telefonního čísla, tak bez souhlasu majitele telefonního čísla se souhlasem soudce (rozhodnutí soudu). K tomuto zjišťování je samozřejmostí využití informačních technologií. Jde opět o využití od prvopočátku věci až do jeho ukončení a jednotlivé informační systémy se prolínají. Uvedu-li smyšlený příklad z praxe, kdy pan Novák vlastní telefonní číslo 777 888 999 v nezjištěném mobilním telefonu a potřebuji zjistit, jaké další telefonní čísla ve stejném mobilním telefonu používá, tak potřebuji nejdříve zjistit IMEI telefonního čísla. Vlastní žádost je vytvořena s využitím již zmiňovaného § 66 zákona č. 273/2008 Sb., ve znění pozdějších předpisů, v informačním systému „Evidence trestního řízení", kdy tuto prostřednictvím buď elektronického formuláře či faxového přístroje odešlu na specializované pracoviště, které v součinnosti s mobilními operátory ustanoví IMEI mobilního telefonu a dále i další telefonní čísla. Toto probíhá v několika databázových skladech nejmenovaných informačních systémů a výstup je opět elektronicky zaslán zpět k požadujícímu útvaru a ke spisové značce, kde je evidován opět v systému „Evidence trestního řízení". Dále podobným způsobem podám žádost na specializované pracoviště společně s rozhodnutím soudce (povolením soudu) k napojení určitého telefonního čísla či určitého IMEI k odposlechu. Po-té je využíván nespecifikovaný informační systém k záznamu dat a k těmto datům je přístup přes tzv. „hardwarový klíč". Díky tomuto „klíči" je záznam dešifrován a přehráván v módu .wmw či jiném. To je jen malá ukázka rozmanitosti a možnostech využití informačních systémů s výše uvedeném paragrafovém znění.

[29] Jelínek J. a kol., Trestní zákoník a trestní řád s poznámkami a judikaturou, 1. vydání, Praha: Leges, 2009, 626 - 627 s, ISBN: 978-80-87212-22-6

6 ZÁPORNÉ STRÁNKY INFORMAČNÍCH SYSTÉMŮ, NÁVRHY NA SYSTÉMOVÉ OPATŘENÍ

Jako každá věc na světě má své klady, které byly zmiňovány na stránkách výše, ale také své zápory či záporné vlastnosti. Při tomto bych začal stejně jako u kladů od vzniku informačních systémů až do dnešní doby.

Již při vzniku jakéhokoliv informačního systému se v testovacím období a kontrolním období zjišťují nedostatky, jak programového vybavení tak náchylnosti systému na napadení hackera a mnoho dalších variant nestability. Tento problém v dnešní době vystává de-facto u jakéhokoliv softwaru i hardwaru. Týká se to i informačních systémů u Policie ČR a určitě i samotné výpočetní techniky, jelikož i u policie funguje emailová pošta, přenáší se a využívají různé soubory z disket, flasch disků či CD/DVD. Toto přináší riziko přenesení viru či napadení spamem programu. Toto platí i u datových skladů určitých informačních systémů. Např. v informačním systému„Evidence trestního řízení“ je velmi často využíváno vkládání souborů, jak grafických, tak např. formáty .EXE archivované v souborech .RAR či .ZIP. Tyto soubory můžou být teoreticky nosiči virů a možného ohrožení samotného datového skladu informačních systémů. V minulosti se již stalo, že např. došlo ke zkopírování části bankovních tajemství v institucích bank a prolomení bankovního tajemství s následnými krádežemi finančních prostředků z účtů klientely či zneužití osobních údajů klientely. Toto teoreticky u policie díky intranetové síti nehrozí, ale praxe je mnohdy jiná než realita a proto zde tento zápor uvádím na prvním místě. Tedy informační systémy a výpočetní technika není v dnešní době 100 % účinně chráněna proti napadení zvenčí. Tomuto mají předcházet např. penetrační testy v bezpečnostní analýze informačního systému, které tvoří důležitou součást bezpečnostní analýzy. Za použití různých nástrojů jsou prováděny pokusy proniknout do různých částí informačního systému zvenčí i zevnitř. Výsledkem těchto testů je odhalení slabých míst v ochraně informačního systému.

„Penetrační testy jsou v podstatě napodobení útoku hackera. Útok může být směrován jak z vnější sítě (typicky z Internetu) na servery umístěné v DMZ (demilitarizované zóně) nebo na vnější rozhraní firewallu, tak i z vnitřku na síťovou infrastrukturu nebo

zranitelné servery. Průnik z vnitřku do systému může být veden fyzicky přítomným hackerem, kterému se podařilo připojit vlastní počítač do interní sítě nebo získat fyzický přístup k počítači ve Vaší síti. Průnik ale může být veden i metodou tzv."sociálního inženýrství průniku", kdy hacker zneužije důvěřivosti uživatele či použije jinou netechnickou metodu a tím získá přístup, který mu samozřejmě nenáleží, nachytá běžného uživatele a podsune mu spustitelný kód, pomocí kterého převezme vládu nad jeho počítačem. Tento přístup pak může využít k získání citlivých dat či vedení dalšího útoku. Útoky pak mohou způsobit tyto škody:

1. *Nedostupnost služby - tzv. DoS či DDoS útoky (Denial of Service či Distributed Denial of Service) - způsobí, že služba, na kterou byl útok veden, přestane obsluhovat legitimní požadavky uživatelů - může dojít i k "zatuhnutí", případně restartu serveru apod.*
2. *Neoprávněný přístup - výsledkem útoku může být situace, kdy útočník získá neoprávněný přístup k zařízení, serveru, službě či datům, a to mu následně umožní provádět neautorizované změny v konfiguraci, mazání nebo modifikaci souborů apod. Často bývá takto napadený server využíván jako základna pro provádění útoků na další zařízení.*
3. *Získání důvěrných informací - výsledkem útoku může být získání citlivých informací - např. seznam uživatelských jmen a hesel, účetnictví, ceníků, mezd apod.*

Penetrační testy tvoří důležitou součást bezpečnostní analýzy. Za použití různých nástrojů jsou prováděny pokusy proniknout do různých částí informačního systému zvenčí či zevnitř. Výsledkem těchto testů je odhalení slabých míst v ochraně informačního systému, uložených dat a infrastruktury testovaného subjektu. Samozřejmě pak následuje definice existujících rizik. Penetrační testy ve své podstatě vyhledávají a aplikují metody pro napadení informačního systému tak, jak by k tomu mohlo potenciálně dojít při projevech počítačové kriminality. Tyto aktivity mají za účel prověřit zabezpečení informačního systému vůči napadení a současně ukázat analyzované organizaci, kde existují slabá místa a kudy může být informační systém napaden. Slabá místa v informačním systému jsou hackery trvale vyhledávána a používané systémy jsou testovány na možnosti napadení. Aby bylo možno čelit jejich

útokům, je nutné velmi podrobně sledovat a testovat informační technologie podobným způsobem.

Při bezpečnostních testech infrastruktury je potřeba se zejména zaměřit na:

1. *penetrační testy vnitřní i vnější (scanning, sniffing, redirecting)*
2. *zkušební útoky*
3. *analýzu zranitelnosti firewallů*
4. *kontrolu bezpečnostních pravidel mezi zónami firewallů*
5. *analýzu zranitelnosti aktivních prvků*
6. *analýzu zranitelnosti operačních systémů na serverech a stanicích*
7. *analýzu systému zálohování*

Testy se provádějí na základě expertních zkušeností metodou "etického hackingu" a ve shodě s normami ČSN ISO/IEC TR 13335 a ČSN ISO/IEC 17799.

Při penetračních testech jsou především prováděny následující zkoušky:

1. *firewally - Dos útoky, změny směrování, zranitelnost*
2. *Backdoory - programy umožňující získání kontroly nad počítačem*
3. *CGI scripty - získání plné kontroly www nad serverem*
4. *DNS systémy - předstíráním identity síťového zařízení*
5. *mailové systémy – spam*
6. *ftp systémy - neautorizovaný přístup k souborovému systému a převzetí kontroly nad serverem*
7. *LDAP systémy - zneužití adresářové služby LDAP (Lightweight Directory Access Protocol)*
8. *síťové odposlouchávání - špatná konfigurace aktivních prvků či nevhodný design infrastruktury umožní síťové odposlouchávání*
9. *NFS systémy - neautorizovaný přístup k souborovému systému a převzetí kontroly nad serverem (Network File System)*
10. *systémy založené na RPC -vzdálené volání procedur (Remote Procedure Call)*
11. *systémy se sdílením zdrojů - získání neautorizovaného přístupu (Samba, SMB)*

12. *SNMP systémy - bezpečnostních díry v implementaci Simple Network Management Protocolu v aktivních prvcích sítě*

Získané znalosti mají další využití pro sledování, testování a výběr nástrojů ochranu před neoprávněným přístupem (Firewall) a pro automatizovanou detekci a zabránění pokusu o napadení informačního systému (Intrusion Prevention System).

Složitým rozhodnutím bývá správný okamžik pro penetrační testy. Řada společností penetrační testy odkládá pod záminkami, jako až bude nový firewall, máme webovou prezentaci hostovanou a do sítě nám přichází pouze emaily, máme čerstvě vybudovaný systém, a ten je přeci v pořádku, máme pravidelně aktualizovaný antivir. To jsou velmi naivní tvrzení, na penetrační testy je čas kdykoliv a je více než vhodné je pravidelně opakovat. Vždyť napadení počítačů a odepření jejich služby může nastat kdykoliv, třeba jen lavinovým rozšířením infikovaného emailu. Nebo třeba zprávou Skype s linkem na kliknutí. Ta přijde od známé a důvěryhodné osoby, a protože komunikace Skype je šifrována, tak nedojde k její kontrole antivirovým programem a hromadné nakažení počítačů je dílem okamžiku. Toto je však možné jen díky neexistenci, či flagrantnímu porušování bezpečnostní politiky. I takovéto situace lze technicky ošetřit, ale bohužel to není běžné.

V případě, že už máte nasazen systém IPS, udělali jste opravdu hodně pro zabezpečení sítě. I když není systém IPS samospasný, je to v dnešní době velmi účinný prostředek pro ochranu a prevenci v síti. Je důležité mít na paměti, že IPS je další částí zabezpečení Vaší sítě. Rozhodně nenahrazuje firewall, antivir či další prvky zabezpečení Vaší sítě. I v takovém případě je ale vhodné udělat penetrační test systému IPS.

Při testech IPS se sleduje především:

1. *Zhodnocení nasazení IPS vzhledem k analýze rizik.*
2. *Zhodnocení procedur pro rekonfiguraci IPS, (false positives, filtry, změna závažnosti signatury).*
3. *Zhodnocení procedur pro aktualizaci signatur.*
4. *Zhodnocení znalostní báze incidentů a procedur pro reportování incidentů.*
5. *Zhodnocení nastavení korelace s ostatními systémy.*

6. *Zhodnocení, kde jsou v síti umístěny kritické prvky a kde chce organizace začít s detekcí.*
7. *Zhodnocení komplexního řešení incidentů.*
8. *Zkušební přenos infikovaného vzorku dat.*
9. *Odolnost na DDoS (Distributed Denial of Service – odepření služby). Tento test je velmi náročný na technické vybavení, útok musí být proveden dostatečným množstvím současně otevřených TCP session a k tomu je potřeba velké množství současně útočících počítačů.*
10. *Konfigurace a způsob vytvoření síťové karantény.*

Výsledky penetračních testů musí být prezentovány ve srozumitelné formě jak pro technické, tak pro řídící pracovníky. Součástí zprávy musí být klasifikace problémů a samozřejmě i doporučení na odstranění zjištěných nedostatků.“[30]

Je zde i zmíněn termín „počítačový virus“ což dle odborné literatury znamená; *„Jako virus se v oblasti počítačové bezpečnosti označuje program, který se dokáže sám šířit bez vědomí uživatele. Pro množení se vkládá do jiných spustitelných souborů či dokumentů. Takový program se tedy chová obdobně jako biologický virus, který se šíří vkládáním svého kódu do živých buněk. V souladu s touto analogií se někdy procesu šíření viru říká nakažení či infekce a napadenému souboru hostitel. Viry jsou jen jedním z druhů tzv. malware, zákeřného software. V obecném smyslu se jako viry (nesprávně) označují i např. červi a jiné druhy malware.*

Zatímco některé viry mohou být cíleně ničivé (např. mazat soubory na disku), mnoho jiných virů je relativně neškodných popřípadě pouze obtěžujících. U některých virů se ničivý kód spouští až se zpožděním (např. v určité datum či po nakažení určitého počtu jiných hostitelů), což se někdy označuje jako (logická) bomba. Nejdůležitějším negativním důsledkem šíření virů je však samotný fakt jejich reprodukce, která zatěžuje počítačové systémy a plýtvá jejich zdroji. Některé viry mohou být takzvaně polymorfní (každý jeho „potomek“ se odlišuje od svého „rodiče“). Viry se na rozdíl od červů sami šířit nemohou.

[30] Stránky Svět sítí (online) 2009 (cit. 2009-11-25 12:05 hod.). Dostupný z WWW: http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=309

Dnes (2007) jsou klasické počítačové viry na jistém ústupu oproti červům, které se šíří prostřednictvím počítačových sítí, hlavně Internetu. Některé antivirové programy se proto snaží chránit počítač i před jinými, nevirovými hrozbami.“[31]

Definovat počítačového viru by měla znít;

„Virus je typ programu, který se dokáže sám šířit tím, že vytváří (někdy upravené) kopie sebe sama. Hlavním kritériem pro posouzení programu jako viru je fakt, že k šíření využívá jiné soubory – hostitele. Virus se mezi dvěma počítači může přenést jedině tím, že někdo přenese celého hostitele, např. nějaký uživatel (obvykle neúmyslně) přenese soubor na disketě či CD-ROM nebo ho pošle prostřednictvím počítačové sítě.“[32]

Jako možná ochrana před napadením hackera či počítačovým virem se lze bránit nejběžněji antivirovým programem, což v dnešní době představuje legálně stažený freewarový program, např. Avast Free Antivirus, který počítač chrání před napadením.

„Antivirový program je počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého software (malware). K zajištění této úlohy se používají dvě techniky:

- *prohlížení souborů na lokálním disku, které má za cíl nalézt sekvenci odpovídající definici některého počítačového viru v databázi*
- *detekcí podezřelé aktivity nějakého počítačového programu, který může značit infekci. Tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné techniky.*

Úspěšnost závisí na schopnostech antivirového programu a aktuálnosti databáze počítačových virů. Aktuální virové databáze se dnes nejčastěji stahují z Internetu.“[33]

[31] Otevřená encyklopedie WIKIPEDIA (online) 2009 (cit. 2009-11-25 v 12:11 hod.). Dostupný z WWW: http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus

[32] Otevřená encyklopedie WIKIPEDIA (online) 2009 (cit. 2009-11-25 v 12:11 hod.). Dostupný z WWW: http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus

[33] Otevřená encyklopedie WIKIPEDIA (online) 2009 (cit. 2009-11-25 v 12:17 hod.). Dostupný z WWW: http://cs.wikipedia.org/wiki/Antivirov%C3%BD_program

A právě poslední věta mne přiměla zmínit další nedostatek a zápor policejních systémů a to, že i ochrana sítí, informačních systémů a datových skladů je založena na výše uvedených principech a tyto principy musí fungovat, nicméně jelikož se jedná již o zmiňovanou uzavřenou síť, musí se též ručně aktualizovat, což je velmi pomalé, vyžaduje toto lidské síly a de facto není 100 % účinné.

Když pomineme nyní napadení hackera nebo útok viru a ponoříme se do problematiky jednotných informačních systémů, najdeme zde mnoho „záporů či nedostatků“, které se budu snažit pojmenovat.

Jedním z hlavních nedostatků je počet přístupů k datovému skladu v jeden okamžik. Je jisté a bude také níže popsané, že jsou určité špičky připojení uživatelů k databázím a na druhé straně určité méně vytížené časy. V nejvíce vytížených časech se často stává, že systémy jsou zpomalené, často vykazují různé chyby, time-outy a v nejhorších případech dojde ke „shození“ serveru a systém je např. 30 minut nedostupný apod.. Dle mého názoru u policie je všeobecně zastaralá výpočetní technika a datové sklady na serverech nejsou výjimkou. V době přechodu na „Evidenci trestního řízení“ byly datové sklady, tehdy ještě na okresní úrovni, dány na již použité či vyřazené servery, které neodpovídali podmínkám provozu, který na nich začal fungovat. Bohužel, toto si nikdo neuvědomil a nebo nechtěl připustit a vzhledem k tomu, že v této době a finanční krizi je málo financí prakticky na všechno se tento problém ani neřešil. Až příchodem 1.1.2008, de facto prvním „pracovním“ dnem nového roku se zjistilo, že systém ETŘ nelze provozovat, protože servery „padají“, databáze tedy nejsou dostupné a celý systém tedy nefunguje. Až po cca 1 měsíci byly nakoupeny nové servery a velkokapacitní disky pro datové sklady a vše začalo až na drobné výjimky fungovat po této stránce jak mělo již od začátku. V tomto ohledu poukazuji na fakt, že někdy rychlost předstihne důkladnost a šetření v důsledku znamená prodražení celé věci.

Pokud se budeme „držet“ nadále informačnímu systému „Evidence trestního řízení“, tato má nepřeberně funkcí a vybrat mezi nimi nějaké záporné vlastnosti je mnohdy těžké, jelikož jedna funkce slouží druhé a následkem toho je, že třetí funguje špatně. Tedy jako příklad bych uvedl, že existuje daný seznam znalců v různých oborech. Tento je rozepsán dle kategorie a jsou zde i správně uvedeny duplicity například – soudní lékařství, toxikologie, kde může vystupovat jeden lékař. Nicméně při

výstupu „Přibrání znalce“, kde systém má vypočítat celkovou částku a další údaje o znalečném dochází k chybným výstupům, jelikož systém počítá např. pitvu poškozeného, která byla oceněna na 12.500,-Kč dvakrát, protože ten samý doktor vystupuje ještě u toxikologie. Pokud se jedná o výstup za krátké období, lze toto napravit ručním dohledáním věci, ale pokud se takto dohledává například celý rok 2009, vychází celková částka mnohdy i o milióny vyšší.

Vzhledem k tomu, že takto by se dalo pokračovat v těchto drobných nedostatcích dále, přešel bych do další úrovně a to je dostupnost informačních systémů. Toto téma se dá rozdělit do podtémat a to uniformovaná policie a služba kriminální policie a vyšetřování a ostatní.

7 SLOŽKY POLICIE ČESKÉ REPUBLIKY A VYUŽITÍ „POLICEJNÍCH IS“

7.1 Uniformovaná policie

Tato složka je nejrozsáhlejší a nejobsažnější u Policie ČR a tedy vznáší nejvíce „požadavků“ na datové sklady jednotlivých informačních systémů v rámci své služby. Bohužel v této době je dostupnost těchto systémů v „terénu“ mimo služebnu velmi problematická. Bohužel dostupnost hifi nebo jinou technologií není dostupná a jedinou možnou lustrací je použití radiokomunikačního zařízení (mobilní telefon nebo radiostanicí). Ne však napřímo, ale přes operační středisko, které lustraci v daném informačním systému provede, jako dotaz pro „jiného oprávněného“. Jako nevýhodu tohoto lze vnímat souvislost s rychlostí lustrace – než policista, který je mimo služebnu, se dovolá na operační středisko, operační důstojník provede vyhledání daného systému a zadá požadavek a podá zpětnou vazbu policistovi, je to velmi dlouhá doba a mnohdy se stává, že informaci potřebuje policista ihned. Pokud by lustrace probíhala v jeho režii, určitě by byla úspěšnost pozitivních výsledků vyšší. Je zde dobré zmínit také bezpečnost zakročujícího policisty, protože je výhodou vidět na fotografii člověka, je výhodou vědět jeho trestní minulost a být na to připraven a toto je velmi těžké tlumočit přes např. mobilní telefon. Tedy v době přelomu roku 2009/2010, kdy již vyspělé technologie jsou k dispozici a není je problém uvést do provozu, policie se potýká

s problémy tipu zastaralé techniky, špatného pokrytí radiokomunikačním systémem. V automobilech nejsou vybavené notebooky, ve kterých by se např. v off-line verzi dalo vylustrovat alespoň to závažné a potřebné a naopak oproti tomu se zavádí technologie bezdrátového placení pokut platebními kartami, které sice přináší určitý komfort především veřejnosti, ale již ne pohodlí a komfort příslušníkovi policie. Jak bylo řečeno, uniformovaná služba plní specifické požadavky služby, tedy má i specifické požadavky na informační systémy. Při pohledu na policistu, který je na služebně a má k dispozici v ideálním stavu svoji výpočetní techniku má de facto stále ty samé požadavky, jako jsou lustrace v trestní minulosti, lustrace osobních údajů, lustrace karty řidiče, dokladů atd.. Bohužel i v této době je praxí ten fakt, že jsou dané nějaké tabulkové přístupy do informačních systémů a i když například policista potřebuje znát detail trestní minulosti a tento detail datový sklad informačního systému má, nemůže se do tohoto dostat, kvůli svým nedostatečným právům přístupu. Já tento fakt vnímám jako velký nedostatek, protože na policistu je kladen nějaký požadavek, co musí prověřit ať již jeho vedoucím nebo závazným pokynem, rozkazem či dokonce normou a on sám tento požadavek nemůže splnit z důvodu již uvedených nedostatečných práv. Nakonec ale opět s využitím telefonní sítě či osobního dotazu na oprávněného pracovníka např. analytického pracoviště výstup z informačního systému dostane do ruky a pracuje s ním. Tedy záporná stránka je ta, že na policistu je požadován nějaký úkon, ale tento on nemůže jednoduše splnit a musí k tomuto využít dalších lidských sil sboru, aby dosáhl výsledku i přesto, že by stačilo specifikovat přístupy jinak. Většinou vedoucí pracovníci oponují tak, že by mohlo docházet k úniku dat a podobně, ale myslím si, že každý policista přísahal služební přísahu a každý policista je zodpovědný za činy, které činí a normalizovat ten je špatný, ten může a ten nemůže je dle mého názoru chybné.

7.2 Kriminální služba a vyšetřování

U pracovníků kriminální služby a vyšetřování dochází k lustracím v informačních systémech také v různých denních či nočních dobách, nicméně tato složka využívá již specifičtější informační systémy, které oproti těm běžným (které ovšem také využívá) jsou méně vytížené a specifické. U těchto se dají také nastavit

specifické přístupy a většinou požadavky určitých policistů kopírují nastavené přístupy. Ale nastává zde opět stejný problém, pokud je policista mimo služebnu. Navíc služba kriminální policie a vyšetřování má k dispozici velmi malý počet radiostanic a tedy jediným možným způsobem lustrace v terénu je buď nelustrovat, což je v té horší variantě a nebo kontaktovat operační středisko nebo kolegy na pracovišti, kteří lustraci, pokud na ní mají oprávnění provedou. Nevýhodou tohoto je specifičnost jednotlivých informačních systémů, do kterých většinou operační důstojník ani nemá přístup. Proto se i v této době stává zvykem používání bloku papíru a tužky a následnou lustrací na služebně. Pokud je lustrace následně pozitivní, může být ale pozdě.

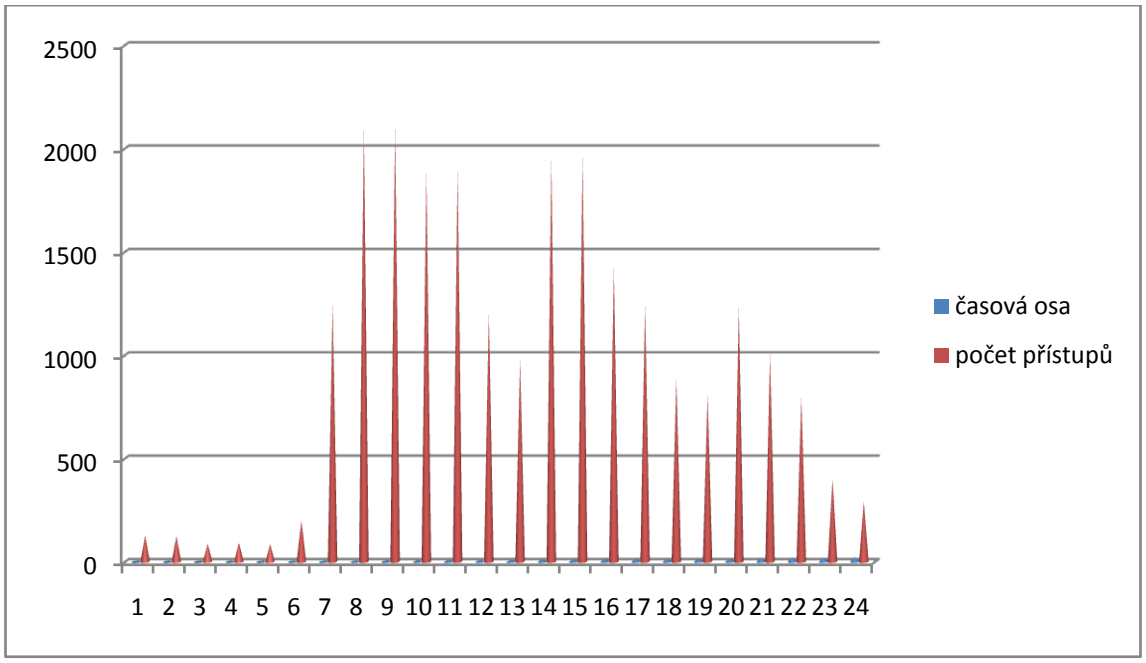
Tedy celkovou nevýhodou a záporem je samotný uzavřený intranet. Pokud by vše běželo na otevřené síti internet, dalo by se např. výše uvedené pokrytí vyřešit, ale na druhou stranu by nastal obrovský problém s hackery, kteří by již měli možnost přímého útoku na datové sklady, ve kterých jsou velmi citlivá data, což není možné a ani reálné, proto sice výše uvádím, že se jedná o zápornou stranu, nicméně i zápor někdy může být kladem.

8 VYTÍŽENOST INFORMAČNÍCH SYSTÉMŮ

Vytížeností jednotlivých informačních systémů se sleduje doba, kdy do jednoho určitého datového skladu nebo několika datových skladů najednou vstupuje určený počet klientů, v našem případě policistů.

U policie platí všeobecné pravidlo u všech informačních systémů a to pravidlo denní pracovní doby, kdy největší počet přístupů je právě mezi 08:00 hod. až 15:00 hod.. Poté se liší ještě dopolední doba a odpolední doba, kdy nejvíce přístupů v jeden okamžik je v době od 08:30 hod. do 11:00 hod, po-té je znatelný pokles přes čas obědů a opět znatelný nárůst v době od 13:00 hod. do 15:00 hod..

V jednotlivých krajích se toto může drobně lišit s ohledem na pracovní dobu, protože v jihočeském kraji se jedná od dobu mezi 07:30 – 15:30 hod., ale např. v Praze se jedná o dobu mezi 08:30 – 17:00 hod.. Níže je graficky znázorněn počet aktivních přístupů do „Intranetu PČR“ v jednom okamžiku v celorepublikovém průměru.

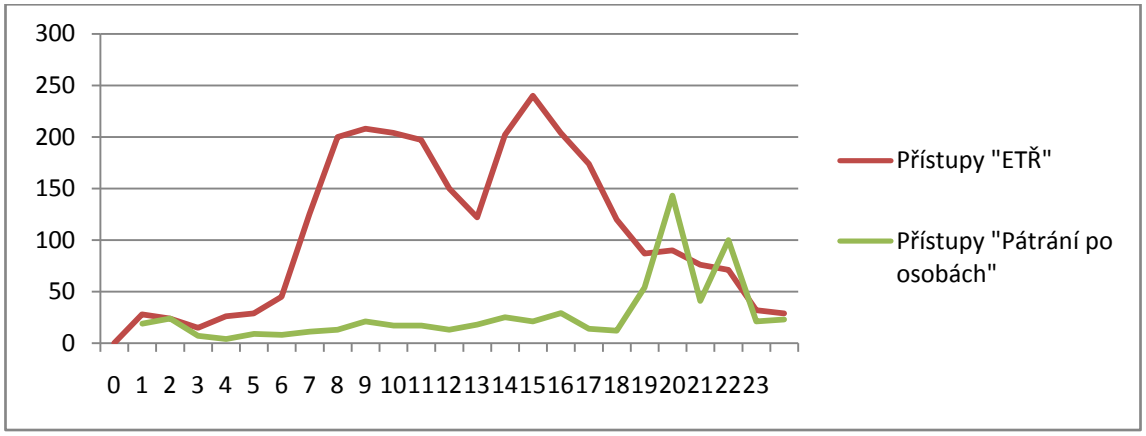


Graf č. 1 – znázornění celorepublikového zatížení sítě intranet PČR aktivními uživateli

Jak je z grafu vidět, nejméně přístupů je v době od 01:00 hod. do 05:00 hod., kdy potřeba lustrací je minimální a práce s informačními systémy není až tak častá. I proto při upgradu jednotlivých databází, či zálohování dat ze serverů se využívají časy po půlnoci. Pokud jde o upgrade týdenní, jedná se o dny z neděle na pondělí a pokud je to upgrade denní, jsou to vždy noční doby okolo 01:00 hodiny ranní. V tuto dobu bývají jednotlivé informační systémy v tom lepším případě maximálně zpomaleny a v tom horším případě zela nedostupné.

Když zde píšeme o vytíženosti informačních systémů, musíme vzpomenout, že nelze porovnávat „obra s trpaslíkem“. Tedy v našem případě např. „Evidenci trestního řízení“, ve které pracuje denně mnoho stovek policistů v jeden okamžik a např. informační systém pátrání – vytěžování, ve kterém se v jeden okamžik dotazuje maximálně desítky policistů a to je ve špičkách provozu. Proto pro porovnání zde uvádím statistické grafy vykazující počet přístupů v jeden okamžik do informačního systému „Evidence trestního řízení“ v Jihomoravském kraji a oproti tomu statistické grafy přístupů v jeden okamžik do informačního systému „Pátrání po osobách“ v celé

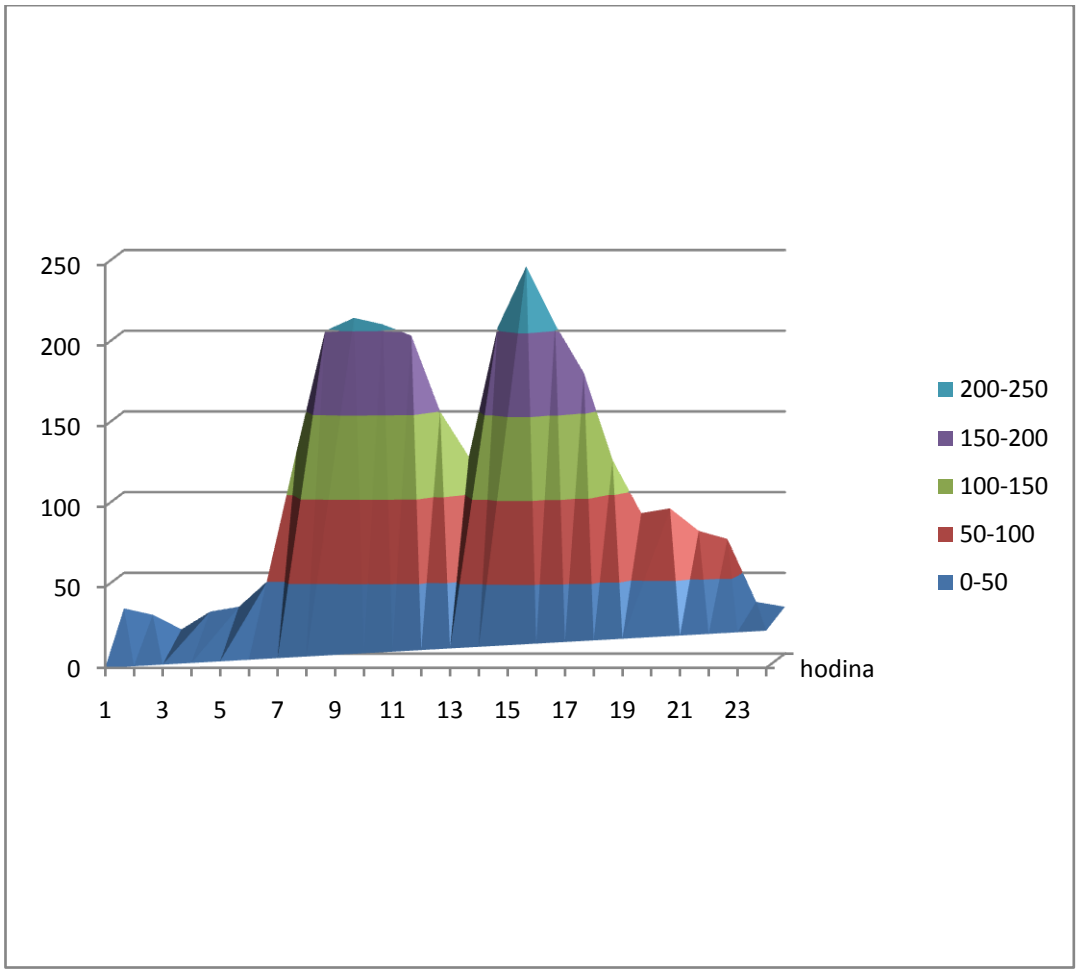
České republice.[34] Je zde znatelný rozdíl přístupů, i když jde o pouze krajskou databázi a tedy do ní můžou vstupovat pouze policisté z krajského ředitelství a z druhé strany jde o celorepublikovou databázi a mohou do ní vstupovat policisté z celé České republiky.



Graf č. 2 – znázornění porovnání krajského přístupu „ETŘ a celorepublikového přístupu „Pátrání po osobách“ v rámci pracovního dne

Zde je znázorněná zajímavost, že v denních hodinách převažuje práce na spisové službě a „krajská Evidence trestního řízení“ jasně překonává v počtech přístupů „celorepublikovou evidenci Pátrání po osobách“, ale v pozdních odpoledních a večerních hodinách dochází více k lustracím mimo služebny a provádí se kontroly osob na ulici v rámci služeb.

[34] Intranet Policie České republiky (offline) 2009 (cit. 2009-11-25 v 14:43 hod.). - http://cportal.pcr.cz/Statistiky.asp



Graf č. 3 – znázornění přístupů krajské databáze „ETŘ“ v rámci pracovního dne

Poslední graf znázorňuje počty přístupů do „Evidence trestního řízení“ v rámci jednoho pracovního dne a zde je znatelný fenomén pracovní doby a je znatelný výrazný pokles uživatelů aplikace v době obědů.

9 VÝZKUMNÁ ČÁST

9.1 Řízený rozhovor s pracovníkem Krajského ředitelství Policie České republiky, Územního odboru České Budějovice, Skupiny kriminální policie a vyšetřování - Analytického oddělení, nprap. Rostislavem Kubouškem

Pro mou bakalářskou práci jsem získal mnoho užitečných informací z řízeného rozhovoru s policistou Policie České republiky zařazeného na Analytickém pracovišti Skupiny kriminální policie a vyšetřování a to nprap. Rostislavem Kubouškem, kdy jsem tomuto položil všechny typy otázek, tzn. otevřené, polootevřené, uzavřené. Většinou však šlo o otázky DICHOTOMICKÉ, VÝBĚROVÉ ČI STUPNICOVÉ.

Řízený rozhovor se zabývá tématy předem volenými a připravenými. Konkrétní dotazy a formulace jsou však řízeny právě probíhající interakcí. Tyto rozhovory jsou dobré pro zjištění zpětné vazby a kladné reakce. Podle dynamičnosti dobrými příklady jsou například talk – show.[35] Byla realizována příprava na řízený rozhovor – polostrukturovaný, samotná realizace byla zohledněna v jednotlivých krocích – začátek, průběh a ukončení. V začátku byl respondent připraven a motivován. Uskutečnění rozhovoru se odehrálo v jeho „domovském prostředí“, kde se respondent cítil „ve svém“ a mohl odpovídat otevřeně a nezaujatě. Byly kladeny připravené otázky, při ukončení rozhovoru byly kladeny upřesňující otázky a v závěru bylo respondentovi poděkováno. Tedy řízený rozhovor měl typickou realizaci.

1) **Od jakého roku pracujete u Policie České republiky?**

Rostislav Kuboušek: „Pracuji u policie již několik desítek let, nerad bych uváděl přesný počet, ale prošel jsem si od hlídkové služby, přes obvodní oddělení, operativu Služby kriminální policie a vyšetřování až k místu, kde nyní sedím a to je Analytické pracoviště

[35] De VITO, J. Základy mezilidské komunikace, 6. vydání Praha: Grada Publishing, 2008, 512 s, ISBN: 978-80-247-2018-8

na našem Územním odboru České Budějovice v rámci Služby kriminální policie a vyšetřování.“

2) **Jak by jste zhodnotil vývoj informačních systémů od jejich prvopočátku, např. při vašem nástupu k zaměstnání u policie až do dnešní doby.**

Rostislav Kuboušek: „Víte, ono se to dá těžko zhodnocovat. Při mém nástupu k policii nebyly krom listinných telefonních seznamů a podobných dokumentů žádné informační systémy. Na to, že to vlastně byly informační systémy jste mne nakonec upozornil vy ve své rozepsané bakalářské práci. Po revoluci v roce 1990 se začala využívat více technika a dokonce začaly být dostupnější počítače a počítačová technika i pro policii jako orgán veřejné moci. Co tím chci říci, není to, že jsme od prvopočátku pracovali na počítačích, tiskli výslechy a podobně, ale že se například začala ukládat data např. otisků papilárních linií pachatelů a neznámých, individuálně identifikovatelných osob. Postupem času v řádech několika let se začaly první počítače dostávat i k nám obyčejným obvoďákům, kteří jsme sloužili na Obvodních odděleních, já konkrétně na Obvodním oddělení České Budějovice. Nicméně první počítač měl vedoucí, kterým jsem nebyl a policie mi laskavě umožnila, abych si usnadnil práci si zakoupit svůj počítač, nicméně ne k lustraci v informačních systémech, protože v té době se již začala rozbíhat např. IS Událost, ale pouze pro psaní textů a výslechů. Až v době, kdy se počítače dostaly na stálé služby se dalo hromadně využívat lustrací v IS. Nicméně i v té době se využívalo spíše specializované pracoviště pro lustrace, které fungovalo 365 dní v roce 24 hodin denně. Mimochodem, toto funguje až dodnes. Abych nemusel rozebírat postupný nárůst počtů výpočetní techniky a tím i rozšíření veškerých informačních systémů, skočím hned do dnešní doby, která se píše od roku 2008, kdy byl nově spuštěn počítačový informační systém IS ETŘ – evidence trestního řízení, ve kterém jsme povinni zpracovávat vše, co je v normálním módu vyšetřování a není nikterak utajené. Utajené věci od stupně vyhrazené se již v tomto informačním systému neevidují a s těmito se nakládá odlišně. Takže abych zakončil myšlenku. Při mém nástupu k policii neexistovalo nic a nyní se vše eviduje, lustruje přes PC, mám minimálně tři přístupová hesla, které musím měnit každé 3 měsíce a vše musím evidovat ve výpočetní technice, respektive v on-line verzích IS a bez počítače neudělám dnes ani krok.“

3) **Jste uživatelem vám přiděleného „pracovního“ PC s přístupem na intranet? Prosím o odpověď ANO – NE.**

Rostislav Kuboušek: ANO

4) **Kolik hodin denně využíváte PC ke své práci v zaměstnání? Prosím, vyberte jednu z možností; 1 – 2 hodiny, 2 – 3 hodiny, 3 – 4 hodiny, 4 – 5 hodin, 5 – 6 hodin, 7 – 8 hodin, více jak 8 hodin.**

Rostislav Kuboušek: více jak 8 hodin denně

5) **K čemu konkrétně vy osobně využíváte informační systémy a co vás první napadne, když se řekne slovo „informační systém?**

Rostislav Kuboušek: „Začal bych druhou částí vaší otázky a to co mi řekne slovo „informační systém“. Abych se přiznal, tak první se naskytne pondělní ráno při zapnutí mého stolního počítače. Nicméně na to jste se asi neptal, takže vážně. Informační systém je pro mne velká pomoc při mé práci, de facto já jako analytik využívám ve výstupech data vkladatelů a jsem na nich životně závislý. Pokud by nebyly informační systémy, nebylo by i mé zařazení, takže když bych to spojil, informační systém se rovná mé práci. No a k čemu konkrétně využívám informační systémy bych zakončil slovem „k výstupům“.“

6) **Spolupracujete s využíváním informačních systémů i s jinými orgány státní správy?**

Rostislav Kuboušek: „Ano, samozřejmě spolupracujeme s Městskou policií v Českých Budějovicích i jiných městech, využíváme jejich kamerové systémy a jejich evidence, ale nejsou to on-line logy do jejich databází, ale musím sepsat oficiální žádost, na kterou mi instituce odpoví. Nejsou to jen Městské policie, ale i úřady, magistráty, Národní bezpečnostní úřad či různorodé firmy.“

7) **Znáte legislativní nástroje, kterými je vymezena součinnost PČR a ostatních subjektů? Odpovězte prosím ANO – NE – NEVÍM.**

Rostislav Kuboušek: ANO

8) **Jakým legislativním nástrojem je vymezena součinnost PČR a ostatních subjektů?**

Rostislav Kuboušek: „Samozřejmě zákonem o Policii České republiky č. 273/2008 Sb. a například u Městské policie České Budějovice zákonem o obecní policii č. 553/1991 Sb..“

9) **Když se vrátím k vaší práci, jakými případy lustrací v informačních systémech se setkáváte nejčastěji?**

Rostislav Kuboušek: „Jsou to hlavně lustrace, které napomáhají k objasňování trestné činnosti a to lustrace dle místa spáchání trestného činu, dle způsobu spáchání, tzv. taktických hledisek spáchání trestného činu a chování pachatele na místě činu, dále lustrace přes specializované pracoviště Policie České republiky u dat mobilních operátorů apod. Blíže bych se nerad vyjadřoval.“

10) **V čem vidíte klady a zápory informačních systémů?**

Rostislav Kuboušek: „ Klady jsou jasné, jsou dostupné odkudkoliv, archiv dat, které nejsou jiným způsobem možné archivovat a zároveň vytěžovat. Zápory jsou také jasné, i když všechny data jsou opatřeny přístupovými hesly a všechny logy jsou archivované, jde o připojení http a jde o uzavřenou síť, jsou možné úniky citlivých dat.“

11) **Jak by jste zhodnotil užitečnost jednotlivých informačních systémů a co by jste navrhoval do budoucnosti?**

Rostislav Kuboušek: „Bohužel na toto vám nejsem schopen odpovědět, protože nejsem analytik, který se zabývá vytížeností a funkčností informačních systémů no a budoucnost, té se spíš obávám než něco plánuji.“

12) **Jste spokojen s kvalitou vedení našeho rozhovoru? Prosím odpovězte ANO – NE – NECHCI ODPOVĚDĚT**

Rostislav Kuboušek: ANO

9.1.1 Dílčí závěr z řízeného rozhovoru

Rozhovor potvrdil mé tvrzení uplatněné v této bakalářské práci, že informační technologie je stále ve vývoji. Na začátku nebylo „nic“ a nyní je na policisty či občanské zaměstnance policie vyžadována dobrá až nadprůměrná znalost informačních systémů a využití informační technologie pro svou práci a že slova „informační technologie“ a „informační systém“ je každodenní záležitostí všech při běžných každodenních činnostech. Potvrzuje se i to, že policista či občanský zaměstnanec policie doslova zůstává „životně“ závislý na výpočetní technice a na informačních systémech a jednotlivých datových skladech.

9.2 Anketa k problematice využívání informačních systémů u Policie České republiky

V této části jsem sestavil anketu se třemi pracovníky Policie ČR, kde jsem se snažil položit otázky týkajících se informačních systémů u Policie České republiky a zároveň jejich využití v praxi jejich služby. Jedná se o policisty zařazené jak u uniformované služby, tj. Krajské ředitelství Policie České republiky, Územní odbor České Budějovice, Vnější služba, Oddělení hlídkové služby, dále Oddělení Dopravní policie - dopravní nehody a dále o policistu Krajského ředitelství Policie České republiky, Územní odbor České Budějovice, Skupina kriminální policie a vyšetřování, linie Obecné kriminality. Modrou barvou jsou vyznačeny odpovědi policisty Oddělení hlídkové služby, červenou barvou pak policisty Dopravní policie, dopravní nehody a zelenou barvou policisty Služby kriminální policie a vyšetřování.

Jste žena či muž ?

- muž
- muž
- žena

Kolik je Vám let?

- 35
- 29
- 42

Kolik let jste zaměstnán ve služebním poměru u Policie ČR?

- 14
- 10
- 19

Říká Vám něco pojem Informační systém v souvislosti s Vaším zaměstnáním?

- ne, vlastně moc ne, jak by to mělo souviset s mým zaměstnáním?
- ano, denně informační systémy využívám při mé práci, jak při výjezdech ve výjezdové skupině dopravních nehod, kde zapisuji údaje do informačních systémů přímo u nehody, tak při práci na spisových materiálech v kanceláři
- ano, vlastně každý den zpracovávám spisovou službu do systému „Evidence trestního řízení“, což by měl být informační systém, dále lustruji v evidenci osob a v dalších informačních systémech mě dostupných

Jak často za den využíváte přístup do jakéhokoliv informačního systému u policie?

- nikdy
- pokud jsem v práci, denně
- jak jsem řekla, denně

Jaký Informační systém využíváte nejčastěji?

- nevím
- Lotus – je to systém evidence dopravních nehod
- Evidence trestního řízení

V jakou dobu nejčastěji využíváte přístupu do Informačních systémů?

- já osobně žádnou, ale vím, že velitel směny něco píše do počítače vždy před a po ranní či odpolední poradě, předpokládám tedy, že využívá informační systémy

- prakticky každou dobu mé služby, ale nejčastěji od 07:00 hod. do 18:00 hod.
- v této době prakticky stále, při výjezdech, při zpracovávání spisových materiálů, nejčastěji ale od 08:00 hod. do 15:00 hod.

Co Vám nejčastěji vadí na informačních systémech PČR?

- jsou málo dostupné a já je nevyužívám, alespoň o tom nevím
- jsou velmi pomalé, protože jsou používány na starých počítačích, jsou natolik „osekané“, že je problém se do nich často dostat a vadí i, že všichni vedoucí vidí, co právě dělám
- jsou pomalé, jsou nepřehledné, v dnešní době je riziko se vůbec někam kouknout a proto mi vadí veškerá monitorace mé činnosti, v nedávné době sem zažila případ, kdy jsem musela zdůvodnit, proč jsem potřebovala fotografii pachatele z Informačního systému registr obyvatel a jak jsem s touto naložila

Co Vám naopak vyhovuje u informačních systémů PČR?

- nevím
- jsou dostupné odkudkoliv a kdykoliv
- můžu pracovat při výjezdu na jakékoliv služebně OOP a nemusím zdlouhavě převážet poškozené k výslechům do Českých Budějovic a zpět, zkracuje to tedy dobu výjezdu a jistě i finanční náklady

Myslíte si, že Informační systém provozovaný policií může předcházet sám o sobě páchání trestné činnosti?

- asi ne, informační systém je program a tento nemůže sám od sebe předcházet trestné činnosti, od toho jsme tady my
- o předcházení trestné činnosti za pomoci informačních systémů, tomu bych rozuměl, ale že by sám informační systém předcházel trestné činnosti, to asi ne, ale v dnešní době je i to možné, ale já o tom nevím
- samozřejmě, napadá mne například systém LOOK, který dohlíží automaticky a automaticky lustruje, zda je vozidlo v pátrání či nikoli a nebo systém kamerových záznamů, například v Českých Budějovicích, kde již samotná přítomnost kamery určité pachatele odrazuje od činu, který by jinak spáchali

Uveďte jednu činnost, kterou vykonáváte dle taxativně vymezených povinností dle § 2, zákona č. 273/2008 Sb. o Policii ČR v souvislosti s informačními systémy.

- pomáhám a chráním
- plním úkoly de trestního řádu
- plním úkoly dle trestního řádu a předcházím páchání trestné činnosti

Domníváte se, že je dostatečně prezentován jakýkoliv informační systém policie?

- ne, nevím o tom
- ne
- bohužel, v této době platí pravidlo, co se nenaučíš sám, jako by nebylo a platí to i u této problematiky

V místě Vašeho pracovního působiště jste spokojen s preventivními opatřeními za pomoci informačních systémů, např. kamerových záznamů?

- vím, že kamerové systémy existují, ale nevím, zda jsou někde ukládány a nebo jsou točeny „live“, proto na tuto otázku nedokážu odpovědět
- ano, ale vždy to může být lepší
- když se ptáte na kamerové záznamy, tyto jsou často nekvalitní, ale je vůbec štěstí, že je máme, takže ano i ne

Co by jste v této problematice změnil?

- určitě větší informovanost, co vlastně existuje
- pokrytí města kamerovými systémy, zvýšení kapacity datových skladů, tak aby zde bylo možné ukládat více informací a zlepšení stavu kvality výpočetní techniky
- určitě bych chtěla zdůraznit, že jsem ráda, co máme, ale do budoucna bych uvítala přehlednější grafické zobrazení všeobecně, dále zabudování hypertextových odkazů do informačních systémů a neposledně i sloučení více podobných informačních systémů do jednoho tak, aby se policista nemusel přihlašovat na 20x

Děkuji za Váš čas a snahu odpovědět v mém rozhovoru.

- děkuji také
- díky
- prosím.

9.2.1 Dílčí závěr - anketa

Z výše uvedeného vyplývá jedna skutečnost, která je na první pohled zřejmá a to, že policista zařazený u Krajského ředitelství policie České republiky, Územního odboru České Budějovice, Vnější služby, Oddělení hlídkové služby ani neví o tom, že by využíval některé informační systémy a neuvědomuje si tu skutečnost, že lustruje v datových skladech jednotlivých Informačních systémů za pomoci radiostanice a operačního střediska. Naopak policista zařazený u Krajského ředitelství policie České republiky, Územního odboru České Budějovice, Vnější služby, Oddělení dopravní policie – dopravní nehody si uvědomuje využitelnost informačních systémů, ale pouze v mezích potřeb svého výkonu služby. Policistka zařazený u Krajského ředitelství policie České republiky, Územního odboru České Budějovice, Skupiny kriminální policie a vyšetřování si vybavuje nejpoužívanější systém Evidence trestního řízení, který denně využívá a je s ním v nejužším spojení. Je ale znatelné, že má celkový přehled a ví, co se je možné v rámci dané problematiky jak po teoretické, tak po praktické stránce využít.

9.3 Dílčí závěr z řízeného rozhovoru a ankety

Z řízeného rozhovoru a anketového šetření lze říci, že většina pracovníků Krajského ředitelství Policie České republiky, Územního odboru České Budějovice ještě dostatečně nezná problematiku informačních systémů u resortu. Je zde velice hmatatelně patrné, u jakého zařazení jednotlivec pracuje. Analytik je v systémech zběhlý a ví „o čem mluví“, naopak policista z Hlídkové služby nevyužívá informační technologie a je zde tedy hmatatelná neznalost daného problému. Tedy je zde do budoucna hodně práce jak na straně programátorů, tak hlavně na straně uživatelů.

ZÁVĚR

Tato práce byla zaměřena na problematiku jak minulosti, tak současnosti i budoucnosti informačních systémů a technologie u Policie České republiky. Práce byla vytvářena z mého vlastního pohledu a byla obohacena o můj subjektivní a praktický pohled, přičemž ne vždy s mými názory lze souhlasit. Je faktem, že téma bakalářské práce není mnoho zastoupeno v literatuře, nicméně proto se snažím ještě více vnést do práce již zmíněný vlastní pohled na věc. V bakalářské práci jsem prezentoval odborné názory, které vycházejí z mé dlouhodobé praxe ve služebním poměru a tyto jsou ověřené vlastní praxí.

V prvopočátcích u policie nebylo využíváno mnoho informačních systémů a vůbec ne automatizovaných. S postupem vývoje informačních systémů se zpožděním byly tyto implantovány do vlastní práce policie, nejdříve okrajově, ale v současné době došlo k masivnímu rozšíření do jednotlivých součástí policie a de facto došlo k tomu, že policie bez výpočetní technologie a hlavních informačních systémů, jako jsou registr obyvatel, registr vozidel, pátrání po osobách, vozidlech či dalších již blíže zmíněných informačních systémů není schopna pracovat. Toto je i jeden z hlavních problémů, kdy cokoliv, ať je to rozmar počasí a výpadek proudu nebo hacker může zabránit kvalitní práci policie jako takové. Nicméně jsem došel k názoru, že v této době již je toto normální a dochází stejně tak k možnosti výpadkům v elektrorozvodných páteřních sítí po celé Evropě stejně jako výpadku bankovních systémů po celém světě.

V této bakalářské práci bylo využito kvantitativních i kvalitativních výzkumných ukazatelů zacílených na zjištění rozdílných znalostí v této problematice a dále k objasnění systemizace jednotlivých informačních systémů. Dále řízeným rozhovorem bylo zjištěno, že u policie jsou zařazeni na systémových místech i odborníci, kteří se zabývají pouze touto problematikou a tedy mohou dosahovat mnohem lepších výstupů z jednotlivých datových skladů než běžně zařazovanými policisty po jednotlivých liniích.

Bylo zjištěno, že u policie je ještě nedostatek kvalitní počítačové techniky a že rozdělování této techniky vázne. V této době je na 100 služebních míst Kriminální policie a vyšetřování v Územním odboru České Budějovice cca 30 míst s novým,

kvalitním počítačem. V ostatních případech nelze využít např. paměťové medium Flash, je využívána stále technologie 3,5“ disketové jednotky. Ke škodě by tedy nebylo konstruktivnější rozdělování výpočetní techniky, dále kvalitnější školení a následná péče o obyčejné uživatele tak, aby mohli z informačních systémů čerpat maximální výstupy.

Dále bych navrhoval zjednodušení přístupových práv do systémů, mnoho dat je skryto, i když jsou k samotné práci potřebné a policista si je stejně např. dožádáním zjistí. Zjednodušila by se tak i zaneprázdněnost specialistů a jistě by se i zmenšili náklad na poštovné či pohonné hmoty. Měla by se tedy projevit snaha o omezení nepolicejních činností, které nejsou nezbytné k využívání datových skladů. Tyto však v této době převládají.

Výše uvedené body by mohly dopomoci ke zkvalitnění práce a spolupráce jednotlivých útvarů a součástí Policie České republiky a vlastní práce policistů. Je vhodné však podotknout, že nyní se úroveň automatizovaných informačních systémů a informační technologie pohybuje na dobré úrovni, rozvíjí se a neustále se zlepšuje. Je to stálý běh činností na dlouhou trať.

SEZNAM POUŽITÉ LITERATURY

Literární zdroje

1. De VITO, J. Základy mezilidské komunikace. 6. vydání Praha: Grada Publishing s.r.o., 2008. 512 s. ISBN: 978-80-247-2018-8.
2. Štraus J. a kolektiv, Kriminalistická technika, 2. rozšířené vydání, Aleš Čeněk, s.r.o., Praha 2008, 128 s, ISBN 978-80-7380-095-6
3. Škoda J., Vavera F., Šmerda R., Zákon o policii s komentářem, Aleš Čeněk, s.r.o., Praha 2009, 397 s, ISBN 978-80-7380-160-1
4. Jelínek J. a kol., Trestní zákoník a trestní řád s poznámkami a judikaturou, 1. vydání, Praha: Leges, 2009, 1216 s, ISBN: 978-80-87212-22-6
5. Halouzka J., Informační bezpečnost: příručka manažera, 1. vydání, Praha: Tate International, 2001, 130 s, ISBN 80-902858-4-8
6. Molnár Z., Automatizované informační systémy, 1. vydání, Praha: Vydavatelství ČVUT, 2000, 126 s, ISBN: 80-01-02269-2
7. Chlachula A., Automatizovaný podnikový informační systém, 1. vydání, Praha: SNTL – Nakladatelství technické literatury, 1990, 225 s, ISBN 80-03-00338-5
8. Kolektiv autorů, Abeceda internetu, 1. vydání, Praha: Computer Press, 2000, 78 s, ISBN 80-7226-369-2
9. Vitovský A., Anglicko-český a česko-anglický výkladový slovník internetu, 1. vydání, Praha: AV Software, 2004, 300 s, ISBN: 80-901428-7-7
10. Zimmelová L., Mladá fronta Dnes – Jihočeské vydání, ročník 18, číslo 1, strana D4
11. Macek P., Bezpečnostní služby, 1. vydání, Praha: Police history, 2001, 196 s, ISBN: 80-86477-03-7

Elektronické zdroje

1. Reboot.cz (online) 2009 (cit. 2009-11-19 12:35 hod.). Dostupný z WWW: http://reboot.cz/obrazky/objmod2.jpg
2. Otevřená encyklopedie WIKIPEDIA (online) 2009 (cit. 2009-11-19 12:35 hod.). Dostupný z WWW: http://cs.wikipedia.org/wiki/Informa%C4%8Dn%C3%AD_syst%C3%A9m
3. Reboot.cz (online) 2009 (cit. 2009-11-19 12:37 hod.). Dostupný z WWW: http://reboot.cz/obrazky/dfd.jpg
4. Reboot.cz (online) 2009 (cit. 2009-11-19 12:39 hod.). Dostupný z WWW: http://reboot.cz/howto/programovani/objektove-orientovane-metody-analyzy/articles.html?id=102
5. Reboot.cz (online) 2009 (cit. 2009-11-19 12:48 hod.). Dostupný z WWW: http://reboot.cz/obrazky/dfd.jpg
6. Otevřená encyklopedie WIKIPEDIA (online) 2009 (cit. 2009-11-19 12:50 hod.). Dostupný z WWW: http://cs.wikipedia.org/wiki/Informa%C4%8Dn%C3%AD_syst%C3%A9m
7. Otevřená encyklopedie WIKIPEDIA (online) 2009 (cit. 2009-11-19 11:30 hod.). Dostupný z WWW: http://cs.wikipedia.org/wiki/Informa%C4%8Dn%C3%AD_syst%C3%A9m
8. Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-19 13:40 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/vozidla/patrani/homepage.php
9. Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-19 13:41 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/vozidla/patrani/index.php
10. Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-19 13:59 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/vozidla/patrani/detail.php?id=22470322090602
11. Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-19 14:26 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/auta/index.html
12. Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-19 14:31 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/vozidla/vozidla/vysledek.php?dotaz=CBU+48-91&akce=vspz
13. Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-19 14:47 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/vozidla/ieud/detail.php?pc=97000374&du=O&cp=s&kp=C&k1=VOJÁK&mx=21&de=3&d0=11.11.2009
14. Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-20 19:51 hod.). Dostupný z WWW: http://aplikace.mvcr.cz/vozidla/ieud/dotaz.php?d0=11.11.2009

15. Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-20 19:58 hod.). Dostupný z WWW http://www.policie.cz/clanek/patrani-po-majiteli-predmetu-patrani-po-puvodu-a-majiteli-predmetu.aspx
16. Oficiální stránky Ministerstva vnitra – Policie ČR (online) 2009 (cit. 2009-11-20 20:12 hod.). Dostupný z WWW: http://www.policie.cz/clanek/patrani-po-majiteli-predmetu-patrani-po-puvodu-a-majiteli-predmetu.aspx
17. Dokument DOHODA O VZÁJEMNÉ SPOLUPRÁCIPŘI ZABEZPEČOVÁNÍ MÍSTNÍCH ZÁLEŽITOSTÍ VEŘEJNÉHO POŘÁDKU vydaná Magistrátem města české Budějovice 09/2009, Oficiální stránky Magistrátu statutárního města České Budějovice (online) 2010 (cit. 2010-02-15 20:27 hod.). Dostupný z WWW: http://www.c-budejovice.cz/cz/mesto/aktuality/Documents/09-08-20_Koordinační%20dohoda%20s%20PČR.pdf
18. Oficiální stránky Katastrálního a zeměměřičského úřadu – Katastr nemovitostí ČR (online) 2009 (cit. 2009-11-23 03:02 hod.). Dostupný z WWW: http://nahlizenidokn.cuzk.cz/
19. Oficiální stránky Katastrálního a zeměměřičského úřadu – Katastr nemovitostí ČR (online) 2009 (cit. 2009-11-22 23:52 hod.). Dostupný z WWW: https://katastr.cuzk.cz/uvod/?enc=windows-1250
20. Oficiální stránky Katastrálního a zeměměřičského úřadu – Katastr nemovitostí ČR (online) 2009 (cit. 2009-11-23 00:24 hod.). Dostupný z WWW: https://katastr.cuzk.cz/rdp/ActionLogIn.do?PAR_LoggedSessionID=0afc666530d642bae9404a954127a900ba96e2bf9a9e&enc=windows-1250
21. Stránky Svět sítí (online) 2009 (cit. 2009-11-25 12:05 hod.). Dostupný z WWW: http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=309
22. Otevřená encyklopedie WIKIPEDIA (online) 2009 (cit. 2009-11-25 v 12:11 hod.). Dostupný z WWW: http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus
23. Otevřená encyklopedie WIKIPEDIA (online) 2009 (cit. 2009-11-25 v 12:11 hod.). Dostupný z WWW: http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus
24. Otevřená encyklopedie WIKIPEDIA (online) 2009 (cit. 2009-11-25 v 12:17 hod.). Dostupný z WWW: http://cs.wikipedia.org/wiki/Antivirov%C3%BD_program
25. Intranet Policie České republiky (offline) 2009 (cit. 2009-11-25 v 14:43 hod.). - http://cportal.pcr.cz/Statistiky.asp

ABSTRAKT

Jakub Šťástka, Informační systémy Policie České republiky a jejich aplikace, bakalářská práce, České Budějovice: Vysoká škola evropských a regionálních studií, o. p. s., 2010, 73 stran. Vedoucí bakalářské práce Mgr. et Bc. Josef Kříha.

Klíčová slova: policie, informační systém, informační technologie, datový sklad, policista, Policie České republiky, Služba kriminální policie a vyšetřování

Informační systémy a informační technologie ve vývoji u Policie České republiky od vzniku až po dnešní dobu. Analyzuje funkčnost informačních automatizovaných i jiných systémů, zkoumá funkčnost prolínavosti a uplatnění jednotlivých informačních systémů v praxi. Snaží se definovat poslání v taxativně vymezených povinnostech policie České republiky. Zkoumá využitelnost jednotlivých informačních systémů a navrhuje pohled do budoucnosti.

ABSTRACT

Jakub Stastka, Police informatic systems of the Czech republic and theire application, bachelor thesis, Ceske Budejovice: Academy of European and Regional Studies, o. p. s., 2010, 73 p. Head thesis Mgr. et. Bc. Josef Kriha.

Keywords: police, information systems, information technology, data warehouse, policeman, Police of the Czech republic, criminal police

Information systems and information technology in the development of the Police of the Czech Republic from conception to the present time. It analyzes functionality of information and other automated systems, it examines the functionality and application of information systems in practice. It tries to define exhaustively defined duties in police of the Czech republic. It examines usefulness of information systems and proposes view into the future.