Webový informační systém pro podporu krizového řízení

Web-based Information System To Support Crisis Management

Bc. Jan Tonner

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan Tonner**
Osobní číslo:	**A11510**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Webový informační systém pro podporu krizového řízení**

Zásady pro vypracování:

1. **Popište schéma operačního a krizového řízení.**
2. **Specifikujte krizové stavy a činnosti odpovědných částí policie.**
3. **Definujte požadavky na webový informační systém.**
4. **Navrhněte hardwarové a softwarové řešení webového informačního systému.**
5. **Specifikujte návaznost informačního systému na jiné systémy policie.**
6. **Zpracujte analýzu rizik řešení postaveného na webové technologii.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **LUBBERS, Peter, Brian ALBERS a Frank SALIM. HTML5: programujeme moderní webové aplikace. Vyd. 1. Brno: Computer Press, 2011, 304 s. ISBN 978-80-251-3539-6.**
2. **SCHURMAN, Eric M a William J PARDI. Dynamické HTML v akci. Vyd. 1. Praha: Computer Press, 2000, xvii, 421 s. ISBN 807226401x.**
3. **MIKLE, Pavol. XDHTML: HTML, XHTML, DHTML : úplná přesná referenční příručka. Vyd. 1. Brno: Zoner Press, 2004, 206 s. ISBN 8086815013.**
4. **VÁCLAVEK, Petr. JavaScript: hotová řešení. Vyd. 1. Brno: Computer Press, 2003, 255 s. ISBN 8072268546.**
5. **FLANAGAN, David. JavaScript: kompletní průvodce. 2. aktualiz. vyd. Praha: Computer Press, 2002, 825 s. ISBN 80-7226-626-8.**
6. **HILLIER, Scot a Daniel MEZICK. Programování Active Server Pages: přel. z angl. orig. Praha: Computer Press, 1998, 291 s.+CD ROM. ISBN 8072261185.**
7. **VIEIRA, Robert. SQL Server 2000: programujeme profesionálně. Vyd. 1. Praha: Computer Press, 2001, xxxii, 1170 s. ISBN 8072265067.**
8. **ŠIMŮNEK, Milan. SQL: kompletní kapesní průvodce. 1. vyd. Praha: Grada, 1999, 247 s. ISBN 8071696927.**

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **22. února 2013**

Termín odevzdání diplomové práce: **22. května 2013**

Ve Zlíně dne 22. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato práce popisuje využívání informačních systémů Policie ČR operačním střediskem a skupinou krizového řízení prostřednictvím webového rozhraní, které následně vede k lepší a rychlejší informovanosti a tedy lepšímu a rychlejšímu řešení krizových nebo mimořádných situací. Především operační středisko, jako složka Policie ČR, která se o mimořádných událostech dozví jako první, musí mít možnost rychlé prvotní reakce na vzniklou situaci, tedy musí mít přístup k potřebným údajům a tyto údaje musí mít rychle a v potřebném rozsahu. První část práce se zaměřuje na teoretický popis náplně jednotlivých zainteresovaných složek a to nejen Policie ČR, vysvětluje a na příkladech demonstruje jednotlivé stavy krize, varianty mimořádných událostí a postupy tzv. krizovými scénáři, kterými se odstraňují následky a minimalizují škody na životech, zdraví a majetku. Dále jsou teoreticky popsány technologie použité pro informační systémy. Ve druhé části se nachází popis jednotlivých informačních systémů provozovaných v rámci Policie ČR, které slouží k rychlému získávání informací potřebných k jednotlivým činnostem při záchranných pracích. Celá práce je vzhledem k rozsáhlosti dané problematiky a nemožnosti charakteristiky všech možných variant mimořádných událostí spíše jen všeobecným popisem práce a využívání interních informací uložených v policejních databázích.

Klíčová slova: krize, mimořádná událost, operační středisko, krizové pracoviště, integrovaný záchranný systém, informační systém, Hypertext Transfer Protocol, HTTP, Active Server Page, ASP, HyperText Markup Language, HTML, Structured Query Language, SQL.

ABSTRACT

This thesis describes the use of information systems of Police by Operations Centre and a group of crisis management through a Web interface which in turn leads to better and faster awareness and thus better and faster solution of emergency situations. The operations center, as part of the Police of the Czech Republic, which is the first to learn about emergency must be able to response to the situation quickly, must have access to the data, and these data must be fast and to the required extent. The first part focuses on the theoretical description of the contents of individual parties involved, not just police, explains and gives examples of individual states of crisis, variants of emergency procedures and the crisis scenario, which removes the effects and minimizes damage to life, health and property . As further the technology used for information systems are theoretically described. The second part is a description of the information systems operated within the PCR, which is used to quickly obtain information needed for individual activities during the relief effort. The whole work is thanks to the magnitude of the problems and inability of characteristics of all possible variants of emergencies rather general description of the work and the use of internal information stored in police databases.

Keywords: crisis or emergency, surgical center, emergency department, an integrated security system, information system, Hypertext Transfer Protocol, HTTP, Active Server Page, ASP, HyperText Markup Language, HTML, Structured Query Language, SQL.

Děkuji Ing. Davidu Malaníkovi, Ph.D. za poskytnutí praktických rad a informací a za odborné vedení při realizaci této diplomové práce.

Rovněž děkuji své ženě a rodině za podporu v průběhu studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD DO PROBLEMATIKY

„V následujících týdnech nemůže být žádná krize, můj diář je již plný“.

Henry Kissinger

Již od dob, kdy se první lidé začali organizovat do vzájemně se podporujících společenských skupin, bylo potřeba řešit náhodně vznikající a neplánované problémy. Ať se již jednalo o ne zrovna klidné soužití s jinými skupinami či překážky způsobené přírodními zákony. V prvopočátcích se vzniklé potíže řešily živelně, tak jak vznikaly, a na odstraňování následků se podíleli zpravidla všichni členové skupiny. Postupně s rozvojem společenských struktur se jednotlivé činnosti dělily do zájmových oblastí a problémy začali řešit specialisté k tomu vyškolení či vycvičení. Starostmi o zásobování potravinami se zabývala jedna skupina, obchodováním jiná, vnější a vnitřní bezpečností opět jiná skupina. Řešením krizových situací se většinou zabývala armáda, která měla na starosti jak vnější tak i vnitřní bezpečnost. Později došlo k rozčlenění těchto oblastí a vytvoření specializovaných složek. Vnější bezpečnost zajišťovala armáda, vnitřní policie, použijeme-li v současnosti užívané názvy. Dnes jsou tyto činnosti rozděleny ještě podrobněji, existují hasičské záchranné sbory, zdravotní záchranné sbory, a jiné složky státu. Všechny mají ale jednu společnou vlastnost. U všech krizových situací asistuje Policie České republiky, ať se jedná o požár, povodně, dopravní nehodu či pád letadla. Prvotním úkolem Policie ČR je zajistit a vymezit prostor krizového stavu a umožnit specialistům (hasičům, zdravotníkům, aj.) nerušený průběh jejich povinností k odstranění či zmírnění dopadu daného krizového stavu.

Pro příklad z minulosti je jedním z prvních dobře zaznamenaných řešení krizových situací požár Říma z doby vlády císaře Nera v roce 64 našeho letopočtu. Řím byl tehdy jako většina tehdejších měst postaven převážně z dřevěných staveb. V té době byla k řešení vnitřního pořádku používána armáda, přesněji pretoriánská garda v počtu několika tisíc později až desítek tisíc jednotlivců, sloužící primárně k osobní ochraně císaře, která sídlila částečně přímo v Římě a částečně v blízkém okolí Říma. Tato garda bojovala s rozšiřujícím se ohněm tak, že preventivně bourala a zapalovala části ulic a bloků a snažila se tak vytvořit nárazníkové pásmo před postupujícím ohněm, aby tak zamezila v šíření a postupu požáru do dalších částí města. V té době standardní řešení bylo později různými dějepisci vykládáno tak, že za požárem stál sám císař označovaný jako šílený. Přitom toto řešení se využívá dodnes například při lesních požárech.

I. TEORETICKÁ ČÁST

1 KRIZOVÉ STAVY

1.1 Krize

Každá oblast lidského konání má svá specifika a svá vlastní pravidla, krizové stavy nabývají různých podob a jejich řešení podléhá specifikům dané oblasti. Krize je těžká situace společenského života nezávislá na vůli člověka vyvolávající potřebu hledání záchrany nebo zabránění neštěstí nebo jeho dopadu. Na druhou stranu krize by bez lidí neexistovaly. Krize má z hlediska hodnotového objektivně subjektivní hlediska, krize jednoho subjektu nemusí být krizí druhého, ale naopak může být i přínosem. Proto může být krize i úmyslně uměle vyvolaná v rámci nějaké strategie či taktiky například v konkurenčním prostředí.

Tedy krize je stav přírodní, společenský, právní, technický atd., který se zásadně liší od rovnovážného stavu a působí negativně až degradačně na celý systém či jen jeho část. Má nepředvídatelný nebo obtížně předvídatelný průběh na velký rozsah společenských aktivit, na životní prostředí, ale i na duchovní hodnoty obyvatelstva. Je to stav, který svým charakterem a negativními následky vážným způsobem naruší chod celého společenského systému nebo jeho části a způsobí selhání dosavadního způsobu fungování subjektu, a predikuje potřebu aplikování speciálních postupů pro obnovu rovnováhy v dané oblasti.

1.2 Krizové stavy a mimořádné události

Dle zákona „č. 240/2000 Sb. O krizovém řízení a o změně některých zákonů (krizový zákon)“ ze dne 28. června 2000 ve znění pozdějších předpisů je mimořádná událost, při níž je vyhlášen stav nebezpečí, nouzový stav, stav ohrožení státu nebo válečný stav.

Stav nebezpečí vyhlašuje hejtman kraje nebo primátor hlavního města Prahy a důvodem vyhlášení je živelní pohroma, ekologická nebo průmyslová havárie, nehoda nebo jiné nebezpečí, při němž je nebezpečí ohrožení životy, zdraví, majetek, životní prostředí nebo vnitřní bezpečnost nebo veřejný pořádek pokud intenzita ohrožení nedosahuje značného rozsahu a není možné odvrátit ohrožení běžnou činností správních úřadů a složek integrovaného záchranného systému. Platí pro území kraje nebo jeho část, doba trvání je nejvýše 30 dnů a případné prodloužení musí schválit vláda ČR.

Nouzový stav vyhlašuje vláda ČR (předseda vlády). Důvodem jsou živelní pohromy, ekologické nebo průmyslové havárie, nehody nebo jiné nebezpečí, které ve značném

rozsahu ohrožují životy, zdraví nebo majetkové hodnoty, nebo vnitřní pořádek a bezpečnost. Platí pro celý stát nebo jeho části a jeho trvání je nejvýše 30 dnů, které v případě nutnosti může prodloužit poslanecká sněmovna.

Stav ohrožení státu vyhlašuje parlament na návrh vlády ČR. Důvodem je bezprostřední ohrožení svrchovanosti státu nebo územní celistvosti státu nebo jeho demokratických základů. Platí pro celý stát nebo jeho části a jeho trvání je neomezené.

Válečný stav vyhlašuje parlament a důvodem je napadení republiky nebo je-li potřeba plnit mezinárodní smluvní závazky o společné obraně proti napadení. Platí pro celá stát a jeho trvání je neomezené.

Orgány krizového řízení jsou vláda, ministerstva, ústřední správní úřady, Česká národní banka, orgány kraje, orgány obce s rozšířenou působností a orgány obce. Jejich činnost řídí již uvedený zákon č. 240/2000 Sb.

1.3 Činnost Policie ČR v případě vyhlášení krize nebo mimořádné události

Mimo uvedené krizové stavy, kdy se v činnost zapojují i články státní správy, Policie ČR řeší nebo se spolupodílí i na mimořádných situacích, které svým rozsahem nepokrývají celá území krajů či státu, ale mají charakter lokální krize. Jsou to například oznámení o uložení či nalezení výbušniny, záchrana pohřešovaných osob s pátrací akcí v terénu, letecká havárie s předpokladem velkého počtu zraněných a obětí, rozsáhlá opatření pro udržení veřejného pořádku v případě demonstrací nebo technoparty, hromadná dopravní nehoda, a mnoho jiných mimořádných událostí.

Veškerá činnost Policie ČR se v případě krizových situací nebo mimořádných událostí řídí platnou legislativou České republiky, ať už se jedná o zákonná opatření, směrnice či nařízení vlády, či interní předpisy Policie ČR.

Policie ČR má pro jednotlivé krizové nebo mimořádné situace vypracovány krizové scénáře, které umožňují efektivně reagovat na vzniklou nebo vznikající situaci. To ve spolupráci s ostatními složkami integrovaného záchranného systému vede k rychlému potlačení nechtěných či nebezpečných stavů.

1.4 Příklady krizových scénářů

1.4.1 Scénář 1. – oznámení o uložení nebo nalezení výbušniny

Průzkum – cílem je zjistit následující informace:

a) druh a množství výbušniny nebo munice či dalších komponentů nástražného výbušného systému,
b) místo uložení a možné působení účinků výbuchu,
c) počet osob nacházejících se v prostoru ohroženého výbuchem a jejich přesné umístění,
d) způsob zneškodnění výbušného systému a jaká je pravděpodobná úspěšnost zneškodnění,
e) charakter činností spojených se zneškodněním výbušného systému (odrušení prostoru, použití kapalného dusíku, trasa pyrotechnického robota, apod.),
f) přítomnost dalších nebezpečných látek v místě zásahu.

Nalezení a zneškodnění nebo zajištění výbušného systému:

a) bezpečnostní pyrotechnická prohlídka místa zásahu,
b) dokumentace místa zásahu,
c) kontrola na přítomnost chemického, biologického nebo jaderného materiálu,
d) zjištění operativních informací k úspěšnému dokončení zásahu,
e) uzavření komunikace pro odvoz výbušného systému.

Zajištění bezpečnosti osob:

a) vymezení nebezpečné zóny a rozhodnutí o režimových opatření pro vstup do nebezpečné zóny, zabezpečení nebezpečné zóny před vstupem nepovolaných osob,
b) vymezení vnější zóny a rozhodnutí o režimových opatření pro vstup do vnější zóny,
c) evakuace osob z nebezpečné zóny na shromaždiště a jejich identifikace,
d) výslech osob za účelem zjištění pohybu dalších osob v nebezpečné nebo vnější zóně.

Regulace dopravy v okolí vnější zóny:

a) regulace pohybu vozidel mimo vnější zónu,
b) zabezpečení volného průjezdu zasahujících vozidel,
c) uzavření komunikací na trase určené pro odvoz výbušného systému,
d) plnění úkolů v oblasti dopravního zpravodajství.

Další možné úkoly na místě zásahu:

a) poskytnutí bezpečnostní a technické podpory ostatním složkám integrovaného záchranného systému,
b) provádění průzkumu ve vnější zóně s cílem nalézt další možné zdroje rizik,
c) asistence při převozu nebezpečných látek z nebezpečné zóny,
d) zajištění veřejného pořádků.

Uvedené postupy vycházejí z všeobecně uznávaných praktik a byly popsány velice obecně. Provádění úkonů zajištění digitálních stop mohou vyžadovat i další alternativní postupy, než byly uvedeny. V případě potřeby se vždy doporučuje konzultovat nastalé situace se znalcem, nebo právním poradcem.

1.4.2 Scénář 2. – záchrana pohřešovaných osob

V případě záchrany pohřešovaných osob se naděje, že pohřešované osoby žijí, vzhledem k času a okolnostem stále zmenšuje. Přesto záchrana pokračuje dle scénáře až do doby, kdy jsou osoby nebo jejich tělesné pozůstatky nalezeny, nebo lze předpokládat, že osoby nalezeny nebudou.

Záchranné práce:

a) získání relevantních informací o možném místě pohybu pohřešovaných osob,
b) stanovení prostoru pro prohledání,
c) soustředění dostatečných prostředků a sil k prohledání stanoveného prostoru,
d) koordinace činností v rámci zásahu Policie ČR se složkami integrovaného záchranného systému,
e) nepřetržité propátrávání stanoveného prostoru s využitím rojnic, kynologů se psi, vrtulníku s termovizí, potápěčů, a podobně, tak, aby se prohledávaný prostor neustále zmenšoval a již prohledané oblasti ze stanoveného prostoru vyloučit,
f) nalezení pohřešovaných osob a zabezpečení lékařské případně první pomoci,

g) zabezpečení transportu pohřešovaných osob do bezpečí,
h) uvědomění zainteresovaných osob, například rodičů či opatrovníků, o nalezení osoby.

Likvidační práce:

a) vyloučit dosud nepropátrané oblasti, u nichž je předpoklad, že se zde pohřešované osoby nenalézají,
b) nasazení sil a prostředků do oblastí s nepřístupným terénem,
c) při nalezení tělesných pozůstatků provést předběžnou identifikaci,
d) provést úkony a postupy k vyloučení možné zaviněné příčiny úmrtí.

1.4.3 Scénář 3. – opatření k zajištění veřejného pořádku při rizikovém shromáždění

Rizikovým shromážděním se zde rozumí například rizikový fotbalový zápas, technoparty, shromáždění či manifestace extrémistických skupin, a podobně.

Příprava na mimořádnou událost:

a) dohoda s obcí, na jejímž území má shromáždění proběhnout, na přítomnosti zástupce této obce, případně jakým způsobem bude zástupce povolán,
b) dohoda se zástupci statutárních orgánů, jejichž přítomnost je potřebná pro provedení policejního zásahu,
c) naplánování prostředků a sil Policie ČR ve spolupráci s integrovaným záchranným systémem, vyčlenění nástupního prostoru pro preventivní přítomnost, tak aby umožnil bezpečný a rychlý příjezd techniky kdykoliv v průběhu shromáždění,
d) způsob vzájemné komunikace a koordinace všech složek zainteresovaných na zásahu,
e) zajištění antikonfliktních týmů pro monitorování mimořádné události či jejího odvrácení, jejichž úkolem je upozorňovat účastníky rizikového shromáždění na nevhodnost či protiprávnost jejich chování,
f) zabezpečení speciálních technických prostředků, jimiž Policie ČR nedisponuje.

Řešení mimořádné události:

a) rozdělení prostoru zásahu na vnitřní sektor, v němž vlastní zásah probíhá, a na sektor vnější uzávěry,
b) nasazení sil do nástupního prostoru,
c) uzavření prostoru zásahu od okolí,
d) poskytnutí sil a prostředků pro zvládnutí zásahu na místě mimořádné události, podpora spojení a koordinace pro ostatní složky integrovaného záchranného systému, například pomoc s vynášením zraněných apod., a to až do doby, kdy je zásah ukončen,
e) povolání zástupce obce nebo statutárních orgánů nezbytných k provedení zásahu,
f) povolání odborníků pro záchranné a likvidační práce, například při nálezu nebezpečných látek, nebo jezdce na koních pro vytlačení osob z chráněné oblasti,
g) získávání operativních informací například formou videozáznamu dokumentační skupinou,
h) řízení dopravy v okolí místa zásahu,
i) ochrana obyvatelstva nacházejícího se v okolí místa zásahu.

1.4.4 Krizové scénáře – sumarizace složek a činnosti odpovědných částí Policie ČR

Pro výkon činností uvedených krizových scénářů je zapotřebí v rámci Policie ČR aktivovat tyto složky:

- **operační odbor** – zajišťuje komunikaci s integrovaným záchranným systémem a realizaci plánů vyrozumění, koordinuje nasazení sil a prostředků Policie ČR, je to vstupní bod mezi policií ČR a obyvatelstvem známým pod telefonním číslem 158,
- **krizové pracoviště** – skupina sloužící pro vnitřní koordinaci resortního systému krizového řízení v případě krizových nebo mimořádných situací,
- **pyrotechnická služba** – zajišťuje odborné úkoly spojené s používáním, vyhledáváním, shromažďováním, prověřování, zneškodňováním, manipulací a přepravou munice, výbušnin, pyrotechnických výrobků, podezřelých předmětů a nástražných výbušných systémů,
- **oddělení technických expertíz** – specializované pracoviště kriminalistického odboru zajišťující daktyloskopii, trasologii, balistiku, genetické zkoumání, apod., zajišťuje veškeré technické aspekty na místě zásahu, pořizuje fotografickou nebo

video dokumentaci, případně analyzuje dokumentační informace z jiných zdrojů, působí jako znalecké pracoviště kriminalistických technik,

- **služba dopravní policie** – zajištění bezpečnosti a plynulosti silničního provozu, vykonávání dohledu nad pozemními komunikacemi, řízení dopravy v oblasti zásahu,
- **služba pořádkové policie** – zabezpečení ohrožené oblasti před vstupem neoprávněných osob, případně jejich vyvedení, zajištění veřejného pořádku, ochrana osob a majetku,
- **služba letecké policie** – zabezpečování letové činnosti pro potřeby útvarů Policie ČR, pátrání po osobách, monitorování velkých oblastí, užití termovize, pořizování dokumentace,
- **služba kriminální policie** – vyšetřování za účelem odhalení pachatelů trestné činnosti, objasňování závažné a organizované trestné činnosti, spolupráce při zjišťování příčin havárií, výbuchů a požárů, zjišťování příčin a podmínek páchání trestné činnosti a spolupráce při jejich odstraňování prováděním opatření preventivního charakteru, zajišťování analytických činností,
- **odbor služební kynologie a hipologie** – psovodi se psy specialisty jsou využíváni k zajištění pátrání po ploše zásahu, detekci omamných a psychotropních látek, detekci výbušnin a akcelerantů, detekci zbraní a jejich částí, pachové identifikace, jezdci na koních zajišťují výkon hlídkové služby, zákroky proti nepovoleným shromážděním osob a srazech extremistických skupin,
- **poříční policie, potápěči** – slouží k plnění specifických úkolů, k vedení zásahu na nebo pod vodní hladinou, poskytují servis ostatním složkám Policie ČR,
- **odbor informačních technologií** – slouží k zajištění technické komunikace zainteresovaných složek, udržuje v provozu celostátní informační systémy, zajišťuje nepřetržitý dohled nad komunikačními trasami, provádí kryptograficky zajištěné přenosy dat a komunikace,
- **skupinu psychologických služeb** – poskytuje psychologickou pomoc osobám z řad veřejnosti zasažených krizovou nebo mimořádnou událostí, intervenci v rodinách pohřešovaných (zejména dětí), napomáhá u výslechů podezřelých či svědků, asistuje u zásahů tam, kde lze očekávat krizovou intervenci, asistuje členům antikonfliktních týmů či vyjednávačům, napomáhají při sdělování nepříjemných zpráv či v jiných obtížných komunikačních situacích.

Z uvedeného je zřejmé, že při jednotlivých krizových činnostech jsou aktivovány téměř všechny složky Policie ČR, některé v průběhu krizové situace, jiné následně po ní. Jejich aktivaci, spolupráci, druh a počet, čas nasazení, a podobně, řídí krizové štáby na základě vývoje dané situace a jsou povolávány v potřebných časových sledech tak, aby vzájemná součinnost byla efektivní a aby nedocházelo k nesouladu mezi jednotlivými složkami.

2 STRUKTURA PRACOVIŠŤ POLICIE ČR

2.1 Operační středisko

Operační střediska jsou vyčleněná pracoviště v rámci Policie ČR zabezpečující v nepřetržitém provozu 24 hodin denně 365 dní v roce plnění bezodkladných policejních úkolů v krizových a mimořádných situacích. Je to to první pracoviště, které se o mimořádné události dozví a které aktivuje ostatní složky Policie ČR v závislosti na druhu a závažnosti dané situace.

Operační střediska vznikala časem postupně na jednotlivých okresech, ale i větších městech, a v letech 2005 až 2006 došlo k zásadní reformě všech těchto pracovišť, kdy se všechna operační střediska soustředila do sloučených pracovišť na jednotlivých krajích. Důvodem byla rozdílná vytíženost, roztříštěnost a nekoncepčnost, kdy některá operační střediska, hlavně ve velkých městech, byla přetížená a jiná přijímala velmi málo hlášení o mimořádných událostech, přesto bylo nutné udržovat na každém operační důstojníky. Reformou bylo vytvořeno 14+1 nových operačních pracovišť, čímž se ušetřil personál a technika. První operační středisko nového typu bylo postaveno v roce 2005 v Brně a vybavení nejmodernější technikou vyšlo přibližně na 35 milionů korun. Jeho pracovníci pokrývají celé území Jihomoravského kraje včetně vlastního města Brna. Postupně byly vybudovány ostatní operační pracoviště na území celé České republiky.

Operační střediska jsou součástí štábních pracovišť, tedy pracovišť vedoucích služebních funkcionářů. Sem spadá policejní prezident, ředitelé útvarů s celorepublikovou působností, ředitelé krajských správ a ředitelé městských celků.

Operační střediska plní služební úkoly spočívající především v poskytování servisu výkonným policejním orgánům a koordinaci sil a prostředků směřujících k zabezpečení relevantních reakcí na vzniklou bezpečnostní situaci v reálném čase v prostoru věcné a územní působnosti, v případě spolupráce s jinými operačními středisky i mimo něj. Základním úkolem je práce s informace, tedy jejich získání, zpracování a reakce na ně. Operační střediska také zajišťují nepřetržité spojení mezi útvary a jeho organizačními prvky, zabezpečují stálý provoz komunikačních zařízení s kryptografickou ochranou. V neposlední řadě je úkolem operačních středisek koordinace činností Policie ČR s integrovaným záchranným systémem, což značí výměnu informací mezi policií, hasičským záchranným sborem a zdravotnickou záchrannou službou.

2.2 Oddělení krizového řízení

Oddělení krizového řízení jsou pracoviště zřízená na jednotlivých krajských ředitelstvích a útvarech s celorepublikovou působností a jejich úkolem je organizace krizového řízení jednotlivých útvarů, plnění krizových, havarijních a obranných úkolů. Zabezpečuje geografickou podporu jednotlivým útvarům a v případě vytvoření krizového štábu pro výkon opatření policejních činností plní i úkoly dokumentační skupiny. Úzce spolupracuje v rámci své působnosti se složkami integrovaného záchranného systému a s bezpečnostními radami krajů, kde se podílí na přípravě podkladů pro jednání a plnění úkolů vzešlých z těchto jednání a tyto následně převádí do havarijních a krizových plánů nebo plánů opatření pro potřeby krizových štábů včetně mapových analýz zainteresovaných oblastí. Tyto plány jsou následně využívány při zvládání krizových a mimořádných situací tak, aby se minimalizovaly škody na životech, zdraví a majetku.

Úkoly oddělení krizového řízení:

- prování analýzu a vyhodnocení bezpečnostních rizik včetně příslušné dokumentace a evidence,
- ve spolupráci s ministerstvem vnitra koordinuje činnosti policie na přípravě a řešení mimořádných událostí a krizových stavů,
- vydává metodiky pro jednotlivé útvary Policie ČR a provádí kontrolu činností na tomto úseku,
- spolupracuje s orgány územních celků, orgánů státních a subjektů hospodářské mobilizace,
- spoluorganizuje vzdělávání a odborná školení policistů v oblasti řešení mimořádných událostí a krizových stavů a vydává vzdělávací plány a učební materiály pro tyto problematiky,
- zastupuje Policii ČR v záchranném integrovaném systému a koordinuje zpracování dokumentace v rámci tohoto systému,
- analyzuje potřeby mobilizačních dodávek a hospodářských opatření pro krizové stavy a podílí se na jejich zajišťování.

2.3 Krizový štáb

V rámci Policie ČR byla zřízena pracoviště, do jejich kompetence spadá řízení případně řešení krizových nebo nenadálých situací. Tato pracoviště kompetenčně spadají přímo pod ředitele územních celků a slouží ke koordinaci jednotlivých článků celé struktury Policie ČR podílejících se na řešení vzniklé mimořádné události nebo krize.

K zajištění operativního řízení a koordinace činnosti útvaru a organizačních článků při plnění úkolů k řešení mimořádných událostí, při hrozbě vzniku krizové situace nebo po vyhlášení krizového stavu byly v každém územním celku či celorepublikovém útvaru zřízeny rozkazem jednotlivých ředitelů krizové štáby. Součástí jednotlivých rozkazů je nejen zřízení krizových štábů, ale i definování jejích členů napříč celou strukturou Policie ČR. Standardními členy krizových štábů jsou ředitelé jednotlivých územních oblastí, náměstci ředitelů jak vnější a vnitřní služby tak i náměstci ekonomičtí, dále vedoucí jednotlivých odborů a to jak přímo tak i nepřímo zainteresovaných, případně ředitelé podřízených územních celků či městských částí. Poslední částí rozkazu je definování rozdělení kompetencí a určení pracovních povinností jednotlivých členů krizového štábu, vydání statutu a jednacího řádu.

2.4 Integrovaný záchranný systém

Integrovaný záchranný systém je souhrnný systém vzájemných vazeb, pravidel spolupráce a koordinace bezpečnostních a záchranných složek státu, orgánů státní správy a samosprávy, fyzických a právnických osob. Slouží pro společné provádění prací záchranného a likvidačního charakteru a přípravě na mimořádné události tak, aby nikdo důležitý či potřebný při pomoci nebyl opomenut a aby si vzájemně nikdo z nich nepřekážel.

Základními složkami integrovaného záchranného systému jsou Hasičský záchranný sbor ČR, jednotky požární ochrany zařazené do plošného pokrytí kraje, poskytovatelé zdravotnické záchranné služby a v neposlední řadě Policie ČR.

Dalšími složkami integrovaného záchranného systému jsou vyčleněné síly a prostředky ozbrojených sil (armády ČR), obecní policie, orgány ochrany veřejného zdraví, havarijní pohotovostní, odborné a jiné služby, zařízení civilní obrany a neziskové organizace a sdružení občanů, které je možné využít k záchranným popřípadě likvidačním pracím.

Integrovaný záchranný systém vznikl v roce 1993 pro potřeby každodenní spolupráce policie, hasičů a zdravotníků při řešení mimořádných událostí, jako například dopravních nehod, požárů, havárií, povodní, atd. Snahou je rychlé a účinné odstranění mimořádné situace, záchrany životů a zdraví, rychlá likvidace následků, v souladu s rozdílnými pravomocemi a pracovní náplní jednotlivých zúčastněných složek a koordinace jejich postupů.

2.5 Plán akceschopnosti

Pro zabezpečení připravenosti a ochrany jednotlivých krajů nebo územních celků se vydává plán akceschopnosti pro plnění úkolů v oblasti krizového řízení. Jedná se především o krizové situace nebo hrozby jejich vzniku a o mimořádné události. Obsahem plánu akceschopnosti jsou postupy řešení těchto událostí včetně zajištění ochrany příslušníků a zaměstnanců před možnými dopady krizových a mimořádných situací a slouží jako podkladový materiál plánů vyrozumění pro svolávání organizačních článků Policie ČR. Za tímto účelem je zřízeno krizové pracoviště standardně umístěné v chráněném objektu v lokalitě nebo oblasti postižené krizí či mimořádnou událostí, odkud se záchranné práce řídí. Dle plánu vyrozumění jsou postupně vyrozumívány a svolávány ty složky Policie ČR, které se podílejí na odstraňování následků událostí. Toto je prováděno koordinovaně tak, aby se maximalizovalo nasazení prostředků jak lidských tak technických v příslušných oblastech kde je jich zapotřebí.

Pro zabezpečení činností útvarů Policie ČR při vzniku hrozby, krizové či mimořádné situace, ale i při obraně státu a pro zajištění ochrany jejich členů podle závažnosti ohrožení pracovníků a areálů mohou být vyhlášeny tyto stupně akceschopnosti:

- **stupeň A** - příprava na spuštění systému krizového řízení nebo jeho částečné spuštění a prověření preventivních opatření,
- **stupeň B** - plná aktivace systému krizového řízení, příprava záložních krizových pracovišť,
- **stupeň C** - částečná evakuace areálů Policie ČR a realizace opatření civilní ochrany,
- **stupeň D** - úplná evakuace areálů Policie ČR, přechod na válečnou působnost a válečnou organizační strukturu Policie ČR.

Jednotlivé stupně akceschopnosti vyhlašuje ministr vnitra nebo jím určený náměstek, ve výjimečných případech policejní prezident nebo ředitel krajského ředitelství policie, takto vyhlášený stupeň akceschopnosti musí být dodatečně schválen ministrem vnitra.

Bez ohledu na vyhlášený stupeň, probíhá v počáteční fázi realizace všech stupňů obdobně.

1. Vyrozumění a uvedení do pohotovosti – prověří se a aktualizuje se plán vyrozumění členů krizového štábu, pověřených pracovníků územních oblastí a organizačních článků.
2. Stanovení pohotovosti – nařídí se pohotovost členů uvedených v předchozím bodě, tito zaměstnanci jsou kontaktováni a aktivováni v předem stanovených časových sledech.
3. Provádění vlastních činností stanovených dle jednotlivých krizových scénářů pro minimalizaci dopadů mimořádných událostí v souladu s ostatními složkami integrovaného záchranného systému.

Všechny činnosti plánu akceschopnosti jsou v pravidelných intervalech cvičně vyhlašovány, aby se odhalily nedostatky. Asi mediálně nejznámější cvičné vyhlašování krizových stavů probíhá v okolí jaderných elektráren, kdy jsou aktivovány nejen příslušné složky Policie ČR a integrovaného záchranného systému, ale i obyvatelé přilehlých obcí.

3 ZADÁNÍ PROJEKTU

3.1 Webový informační portál

Informační systémy založené na webové technologii jsou online komunikací a prezentací v rámci sítě ať již celosvětového Internetu, nebo v našem případě uvnitř firmy či státní správy. Tato komunikace umožňuje směřování informací dle potřeb jednotlivých uživatelů, kdy údaje předkládané zaměstnancům mají formu odkazů, dokumentů, obrázků, prezentací a dalších jiných typů souborů. Velikou výhodou webového řešení je, že uživatelé se k informacím dostanou z jakéhokoliv počítače připojenému k dané síti a nemusí mít nainstalovány speciální programy. Trendem dnešní doby je snaha o rozšíření služeb, maximalizace a konsolidace informací do jedné stránky, tedy nabídka komplexního servisu včetně zpětné vazby.

V případě, že je možné identifikovat připojeného uživatele, je následně jednoduché upravit tomuto uživateli skladbu informací a i činnosti, které mu přísluší, a potlačit nebo dokonce znepřístupnit nedovolené údaje nebo části aplikací. V případě informačního systému provozovanému v rámci rezortu Policie ČR je povinností každého uživatele doménové přihlášení, čímž je identifikace zaručena.

3.2 Požadavky na webový informační systém pro podporu krizového řízení

Cílem je vytvoření jednotného informačního systému rozděleného do zájmových modulů, který umožní v rámci přesně definované organizační struktury zaměstnancům krizových pracovišť a operačních odborů získávat informace potřebné pro jejich činnost při zvládání krizových a mimořádných událostí a zrychlit tok informací, čímž dojde k rychlejší reakci na nenadálé situace. Veškeré informační systémy budou zpřístupněny formou webového rozhraní na prostředcích Policie ČR bez nutnosti dalších investic do výpočetní techniky či programového vybavení a na stávající vnitřní intranetové síti oddělené od internetu, ke které mají přístup všichni zaměstnanci tohoto rezortu.

K přístupu k informačnímu systému bude využito doménového přihlášení (identifikace uživatele), kdy každý uživatel již má vytvořen účet v policejní doméně provozované na Active Directory, tedy bude využit již existující a provozovaný stav.

Informační systém „*Plán vyrozumění*“ bude umožňovat vytvoření skupin uživatelů dle pořadí vyrozumění, editovat tyto skupiny a jejich pořadí, pořizovat výstupy jednotlivých skupin formou tiskových výstupů, definovat práva přístupu k datům a kontrolovat úplnost dat v systému, případně prostřednictvím jednotlivých vedoucích pracovníků zjednávat nápravu.

Tiskové výstupy jsou nutné pro situace, kdy dojde k výpadkům dodávky elektrické energie a tím i nemožnosti práce s výpočetní technikou. Tiskové výstupy se budou dělat pravidelně v intervalech určených jednotlivými krizovými pracovišti dle jejich potřeb a budou uloženy v papírové formě v zabezpečeném prostoru, obvykle v trezoru, aby se zabránilo případnému úniku osobních informací mimo pracoviště krizového řízení nebo operačního střediska.

Informační systém bude provázán s těmito aplikacemi:

- administrace organizační struktury umožňující definovat postavení jednotlivých uživatelů v rámci hierarchické struktury Policie ČR,
- administrace osobních údajů jednotlivých uživatelů, pomocí které si jednotliví uživatelé spravují své osobní, kontaktní a jiné informace,
- veřejný výstup kontaktů a organizační struktury formou výpisu seznamů či vyhledávání, kde jsou potlačeny informace neveřejného nebo soukromého charakteru, a který je využíván všemi zaměstnanci Policie ČR k rychlému zjištění potřebných údajů,
- aplikace elektronické správy a přidělování dokumentů s možností prokazatelného seznámení uživatelů s jednotlivými přidělenými dokumenty, pomocí nějž se distribuuje veškerá dokumentace jednotlivým uživatelům či celým skupinám uživatelů.

Celý informační systém umožní komfortní a uživatelsky příjemný přístup k uloženým informacím a snadnou správu dat dle přidělených oprávnění, aplikace by měla být intuitivní a měla by zachovávat principy pro práci s podobnými programy.

Použité technologie budou založeny na produktech Microsoft. Jde především o Internetovou informační službu 7 a databázový systém Microsoft SQL 2008. Všechny aplikace budou koncipovány pouze pro Internet Explorer verze 6 a vyšší, neboť v rámci Policie ČR nejsou jiné alternativní webové prohlížeče povoleny.

3.3 Standardní instalace počítače u Policie ČR

Každý počítač, ať nový či již použitý, je před předáním zaměstnanci k užívání kompletně smazán (zformátován) a je na něm provedena standardní instalace softwarových produktů. V případě použitých počítačů, kdy dochází k předání od jednoho uživatele k jinému, je počítač před kompletním vyčištěním odzálohován a záloha je uložena do datového úložiště po dobu několika měsíců. Tímto způsobem je zabráněno nechtěnému smazání důležitých dat, neboť sami uživatelé si neuvědomují důležitost uložených údajů a předchází se takto situacím, kdy uživatel předávající počítač si po celkovém vyčištění počítače vzpomene, že si sám neprovedl zálohu pro něj potřebných souborů. Standardní dobou uložení zálohy je půl roku, po této době jsou archivovaná data nenávratně smazána.

Na uživatelský počítač jsou standardně nainstalovány tyto programy:

- operační systém Microsoft Windows verze XP nebo 7,
- kancelářský balík Microsoft Office 2003 nebo 2007,
- Internet Explorer verze 6 a vyšší, jež je součástí operačního systému,
- Adobe Reader verze 5 a vyšší pro práci s uloženými dokumenty.

Další programy či aplikace jsou instalovány již dle specifických požadavků jednotlivých odborů, skupin či uživatelů na výkon jejich pracovních povinností a nejsou standardní výbavou počítače. Jedná se především o programy pořízené a schválené pro provoz na počítačích Policie ČR, které jsou licencovány buď celorepublikově nebo v rámci jednotlivých krajů či územních celků.

Na uživatelských počítačích Policie ČR není dovoleno instalovat a používat software, který nebyl schválen pro provoz a který neprošel typovou registrací. Typovou registrací se rozumí soubor činností, které vedou k důkladné kontrole jak z pohledu funkčnosti, tak z pohledu bezpečnosti a v neposlední řadě i licenční politice výrobce. V okamžiku potřeby nějakého nového software jsou nalezeny odpovídající programy, které se v rámci legální licenční politiky nainstalují na zkušební policejní techniku na pracovišti policejního prezídia. Zde se kontroluje činnost programu tak, aby odpovídala požadavkům jak funkčním, tak i bezpečnostním. Po testech dojde k rozhodnutí, který program bude nadále využíván na počítačích Policie ČR a je vydáno rozhodnutí o typové registraci. Vybraný software je pořízen a je vydáno doporučení o jeho používání, ostatní programy jsou ze zkušebních počítačů smazány. Tímto způsobem je docíleno jednotnosti všech

softwarových produktů na všech počítačích v rámci Policie ČR. Například pro provoz na počítačích Policie ČR byl jako webový prohlížeč vybrán Internet Explorer od společnosti Microsoft a jiné alternativní webové prohlížeče byly zakázány.

3.4 Hardwarové a softwarové řešení

Jedním z požadavků na provozování informačního systémy bylo využití takové výpočetní techniky a technologie, která nebude pro Policii ČR znamenat další investice. Z toho důvodu byly všechny jednotlivé aplikace navrženy pro využívání protokolu HTTP (Hypertext Transfer Protocol), jenž je zpracováván všemi počítači se standardní instalovanou softwarovou výbavou a to operačním systémem Windows spolu s Internet Explorerem, který je součástí operačního systému. Servery, umístěné na centrálním pracovišti v Praze, mají nainstalovány Internet Information Services podporující tento protokol a umožňující vyvíjet a provozovat aplikace na technologii HTML (Hypertext Markup Language) a ASP (Active Server Pages) s využitím databázového prostředí SQL (Structured Query Language). Servery jsou připojeny na vnitropodnikovou intranetovou optickou síť 10 Gbit, zajišťující v rámci Policie ČR velmi dobrou rychlost a prostupnost požadavků připojených uživatelů. Vnitřní intranetová podniková síť je striktně oddělena od celosvětové Internetové sítě.

Aplikace a data jsou umístěny na centrálním pracovišti v Praze na samostatných serverech:

- webové aplikace ASP – Blade server Hewlett Packard HP BL680c se čtyřmi procesory Intel Xeon, RAM 30 GB, HDD 1TB, 64 bitový operační systém Windows Server Enterprise SP2, Microsoft Internet Information Services 7,
- databázové prostředí SQL – Blade server Hewlett Packard HP BL680c se čtyřmi procesory Intel Xeon, RAM 30 GB, HDD 1TB, 64 bitový operační systém Windows Server Enterprise SP2, Microsoft SQL server 2008 R2.

3.4.1 Protokol HTTP a HTTPS

Internetový protokol HTTP (Hypertext Transfer Protocol) je určen pro přenos dokumentů ve formátu HTML využívající obvykle port TCP/80 a funguje metodou dotaz – odpověď. Klient prostřednictvím internetového prohlížeče odešle na server dotaz ve formě prostého textu a od serveru obdrží odpověď, která je uživateli opět prostřednictvím internetového prohlížeče prezentována na jeho monitoru. Protokol HTTP je bezestavový, což znamená,

že server poté co zpracuje a odbaví požadavek klienta, zapomene na proběhlou komunikaci a případný stejný dotaz zpracuje a odbaví pokaždé stejným způsobem.

Nevýhodou protokolu HTTP je přenos dotazů a odpovědí v prostém textu bez jakéhokoliv zabezpečení. Proto je tento protokol, v případě potřeby, nahrazen protokolem HTTPS (Hypertext Transfer Protocol Secure), který probíhající komunikaci šifruje metodou SSL/TSL (Secure Sockets Layer / Transport Layer Security) a zamezí tak případným odposlechům komunikace mezi serverem a klientem.

Příklad komunikace:

Dotaz z prohlížeče uživatele na stránku www.seznam.cz:

GET /index.html/ HTTP/1.1

Host: www.seznam.cz

Connection:close

User-Agent: Opera/9.80 (Windows NT 5.1; U; cs) Presto/2.5.29 Version/10.60

*Accept-Charset: UTF-8,**

[prázdný řádek]

Odpověď serveru na dotaz:

HTTP/1.0 200 OK

Date: Fri, 15 Oct 2004 08:20:25 GMT

Server: Apache/1.3.29 (Unix) PHP/4.3.8

X-Powered-By: PHP/4.3.8

Vary: Accept-Encoding,Cookie

Cache-Control: private, s-maxage=0, max-age=0, must-revalidate

Content-Language: cs

Content-Type: text/html; charset=utf-8

Po této hlavičce následuje jeden prázdný řádek označující konec hlavičky a poté je již uveden požadovaný HTML dokument. V hlavičce odpovědi je uvedeno, že dotaz byl úspěšný, datum a čas vyřízení dotazu, informace o serveru, který dotaz zpracoval a informace o typu vráceného dokumentu.

3.4.2 Jazyk HTML

Značkovací jazyk HTML (HyperText Markup Language) je určen pro formátování stránek v prostředí internetu a umožňuje publikování dokumentů v tomto prostředí. Je přenášen protokolem HTTP formou prostého textu ze strany serveru do počítače klienta. Pomocí prohlížeče obsahujícího HTML je tento prostý text formátován na monitor už ne jako shluk znaků, ale jako upravený dokument. Toho je dosaženo pomocí formátovacích elementů tagů, které definují vzhled a umístění jednotlivých objektů v dokumentu. Příchozí prostý text ze strany serveru je postupně podroben analýze a je rozložen na jednotlivé elementy. Ty jsou poté vyhodnoceny, jednotlivým elementům je přiřazen způsob zobrazení, a poté je celý dokument zobrazen na monitoru uživatele. Všechny popsané činnosti HTML jsou provedeny na počítači klienta, server na tuto činnost nemá žádný vliv, a zobrazení dokumentu je závislé na použitém webovém prohlížeči, případně jeho verzi. Jazyk HTML podporuje dynamické chování dokumentu na počítači klienta prostřednictvím skriptovacího jazyka JavaScript, který umožňuje interaktivní manipulaci uživatele s obsahem HTML stránky, a kaskádových stylů CSS umožňující popsat způsob zobrazení stránek. Stránka prezentována v HTML formátu má příponu *.html* nebo *.htm*.

Standardní HTML dokument má předepsanou strukturu, začíná tagem *<HTML>* a končí *</HTML>*. Uvnitř těchto dvou tagů se nachází vlastní dokument, který je rozdělen do dvou částí a to hlavičky a vlastního obsahu HTML dokumentu. Hlavička je označena tagy *<HEAD>* a *</HEAD>* mezi nimiž se nachází pro uživatele nezobrazované interní informace dokumentu, jež jsou potřebné pro webový prohlížeč. Jsou zde uvedeny metatagy, což jsou informace například o jazyce, znakové sadě, odkazy na soubory se skripty či styly, apod. Údaje uváděné v hlavičce nemají povinný charakter, pokud je údaj uveden, pak je uplatněn, pokud údaj uveden není, webový prohlížeč si v případě potřeby upraví zobrazení dle vlastního defaultního nastavení. Například metatag *<link href="styl.css" REL="STYLESHEET" TYPE="text/css">* odkazuje na externí soubor s kaskádovými styly. Při zobrazení HTML dokumentu se webový prohlížeč pokusí soubor styl.css najít a uplatnit. V případě neexistence tohoto souboru, či jeho chybné vnitřní struktuře, webový prohlížeč nenahlásí chybu ani nezkolabuje, ale veškeré požadavky odkazující se na daný soubor nahradí vlastním defaultním nastavením. Vlastní obsah HTML dokumentu se nalézá mezi tagy *<BODY>* a *</BODY>*. Zde je definována vlastní stránka, tedy to, co se uživateli zobrazí na monitoru. Tělo HTML stránky obsahuje veliké množství formátovacích tagů, kterými se ovlivňuje vzhled, umístění, či jiná funkcionalita

jednotlivých objektů ve webovém prohlížeči. Například tag *<A tref="www.seznam.cz">Seznam</A>* vykreslí do stránky klikací odkaz na webový portál „Seznam.cz“, *<CENTR>Text</CENTR>* vycentruje na řádku uvedený text, *<B>Text</B>* zobrazí uvedený text tučným písmem. Možností využití HTML jazyka je nepřeberné množství a není cílem této práce je všechny popsat.

3.4.3 Skriptovací jazyk JavaScript

Jazyk JavaScript je objektově orientovaný multiplatformí programovací jazyk, využívaný pro HTML stránky. Je standardně vkládán přímo do HTML stránky buď formou přímého vykonávání, nebo formou funkcí uvedených v hlavičce dokumentu. Slouží k interaktivnímu ovládání uživatelských prvků, jako jsou různá tlačítka, textová vkládací pole, různé animační prvky či efekty k obrázkům. Jeho možnosti jsou v důsledku bezpečnosti omezeny tak, aby neohrozily uživatelský počítač, například nemůže pracovat se souborovým systémem počítače, na němž byla HTML stránka s JavaScriptem spuštěna.

Příklad užití JavaScriptu: Mějme v HTML stránce obrázek. Když na tento obrázek najede kurzor myši, dojde k výměně daného obrázku za jiný. Když se kurzor myši z obrázku vzdálí, dojde k zobrazení původního obrázku. V HTML stránce bude uveden řádek:

<IMG src="obr1.jpg" onmouseover="this.src='obr2.jpg'" onmouseout= "this.src='obr2.jpg'">

IMG je tag označující vložení obrázku do stránky HTML, parametr *src* definuje cestu k obrázku na webovém úložišti, parametr *onmouover* je JavaScriptový konstrukt reagující na událost najetí kurzorem myši na obrázek, *this.src=obr2.jpg* nahrazuje původní obrázek novým obrázkem, *onmouseout* je konstrukt reagující na událost opuštění kurzoru myši daný obrázek, *this.src=obr1.jpg* nahrazuje nový obrázek původním. Uvedený příklad není pro vlastní činnost HTML stránky podstatný, ale zvyšuje uživatelský komfort a celkový vzhled stránky, uživatel vidí interaktivitu stránky, se kterou pracuje, a ví, že stránka reaguje.

Každá HTML stránka může mít svůj vlastní JavaScript, ale jsou zcela běžné případy, kdy definovanou funkci využívá více stránek. Je možné vlastní skript uvést do každé stránky samostatně, nebo lépe vytvořit pouze jednu funkci a tu dát k dispozici více stránkám. V tom případě se JavaScripty vytvoří v samostatném souboru, který je poté do HTML stránky do sekce HEAD vložen odkazem *<SCRIPT src="skripty.js"></SCRIPT>*. Výhoda

tohoto řešení spočívá v lepší správě skriptů, kdy úpravou JavaScriptu na jednom místě dojde k okamžitému promítnutí do všech návazných HTML dokumentů.

3.4.4 Kaskádové styly CSS

Kaskádové styly CSS (Cascading Style Sheets) jsou jazyk pro popis zobrazení objektů umístěných v HTML stránce a smyslem bylo oddělit strukturu a obsah stránky od jejího vzhledu. Vzhled jednotlivých objektů je definován na jediném místě, na něž se dané objekty pouze odkazují. Není tedy potřeba definovat všechny stylové parametry u každého objektu zvlášť. Tímto způsobem se dá snadno dosáhnout jednotného vzhledu celých webových portálů, bez neustále se opakujících stylových definicí, což v konečném důsledku šetří čas programátorům. Definici lez provést jak u jednotlivých tagů, tak v HTML stránce v sekci HEAD, ale podobně jako u JavaSciptu je možné všechny styly uvést v externím souboru.

Příklad nastylování textu přímou definicí u tagu:

<DIV style="font-family:MS Sans Serif;font-size:10pt;color:#000000;text-align:justify">Text</DIV>

style parametr obsahuje seznam uplatněných stylů, *font-family* nastavuje písmo, *font-size* velikost písma, *color* barvu písma, *text-align* způsob zarovnání písma v odstavci. Takto by bylo možné nadefinovat styl u všech textů v rámci HTML dokumentu, nevýhodou je opakování definování u jednotlivých objektů. Pro stejné objekty je vhodnější použít definici v hlavičce dokumentu, tu pojmenovat a jednotlivé tagy pouze odkázat na pojmenovaný styl:

<STYLE>

.jmeno { font-family:MS Sans Serif;font-size:10pt;color:#000000;text-align:justify }

</STYLE>

nebo uvedení souboru s externími styly

<link href="styly.css" REL="STYLESHEET" TYPE="text/css">

pak vlastní odkaz na styl v rámci tagu

<DIV class="jmeno">Text</DIV>

Výhodou definování globální stylů v externím souboru je, podobně jako u externích JavaScriptů, jednoduchá a přehledná správa vzhledových informací. Změnou parametrů v jediném externím souboru stylů se dosáhne změny vzhledu celého webového portálu.

3.4.5 Jazyk ASP

Skriptovací jazyk ASP (Active Server Pages) je určen pro dynamické zpracování stránky na webovém serveru. Na rozdíl od statické stránky, kterou server bez jakékoliv další činnosti pouze odešle uživateli, je dynamická stránka před vlastním odesláním nejdříve vytvořena a teprve poté je jako HTML dokument klientovi odeslána. Toho je často využíváno například pro práci s datovými úložišti, kdy je vygenerována tatáž stránka pouze s rozličnými údaji na základě požadavků klientů lišících se v nějakém definovaném parametru. Standardně jsou ASP skripty uvedeny v souboru s příponou *.asp*.

ASP skripty se vkládají přímo do HTML dokumentu mezi značky <% a %>. V průběhu zpracování ASP stránky vyžádané klientem nejdříve webový server vyhodnotí skript uvedený mezi značkami, dané místo nahradí výsledkem vyhodnocení a klientovi je předána již jen prostá HTML stránka bez ASP skriptů.

Příklad ASP kódu a HTML odpovědi:

ASP kód:

```
<%
for i=1 to 5
        response.write „Řádek č. “ & i & „<BR>“
next
%>
```

HTML kód odeslaný klientovi:

Řádek č. 1

Řádek č. 2

Řádek č. 3

Řádek č. 4

Řádek č. 5

kde *for i=1 to 5* a *next* je programová smyčka, která 5 krát bezprostředně po sobě vykoná kód obsažený uvnitř smyčky, *response.write* je příkaz, který vypíše na monitor parametr uvedený za tímto příkazem.

3.4.6 Jazyk T-SQL

Standardizovaný dotazovací jazyk SQL (Structured Query Language) se využívá pro práci s daty v relačních databázích. Jeho účelem je jednoduchou formou spravovat a prezentovat data uložená v datovém úložišti. Relační databáze jsou dnes nejrozšířenější formou uchovávání dat, kdy jdou uložené údaje koncipovány formou vzájemně (relačně) propojených tabulek. Jazykem SQL (T-SQL) lze s daty manipulovat a jednoduchou formou prezentovat, tedy poskytovat uložené údaje jiným aplikacím v našem případě dynamickým stránkám ASP.

Jazyk SQL obsahuje všechny standardní příkazy a funkce k definování a manipulaci s daty, řízení přístupových oprávnění k datům, příkazy pro správu a řízení transakcí, apod. Toto lze rozdělit do několika základních skupin:

- příkazy pro definici dat – CREATE, ALTER, DROP, …,
- příkazy pro manipulaci s daty – INSERT, UPDATE, DELETE, SELECT, …,
- příkazy pro řízení přístupových oprávnění – GRANT, REVOKE,
- příkazy pro správu transakcí – START TRANSACTION, COMMIT, ROLLBACK,
- příkazy pro řízení běhu programu – IF, CASE, WHILE, …,
- funkce pro manipulaci s uloženými daty - AVG, SUM, MIN, MAX, COUNT, RTRIM, LTRIM, LEN, SUBSTRING, UPPER, LOWER, …

Příkazů, funkcí, procedur, … je nepřeberné množství svým rozsahem přesahující popis a rozsah této práce.

SQL umožňuje formou uložených procedur a funkcí předem definovat celou strukturu příkazů, uzavřít je do pojmenované virtuální podoby a ve vhodných programátorem definovaných okamžicích je volat. Uložené procedury a funkce jsou v SQL uloženy v optimalizované podobě, čímž je jejich vykonání rychlejší. Další nezanedbatelnou výhodou těchto struktur je bezpečnost použití, kdy je určitý sled programových kroků přesně definován a bez detailní znalosti vnitřní struktury procedury nebo funkce je těžké odhalit, jakým způsobem procedura nebo funkce dosáhne výsledku, tedy jak získá data z relačních tabulek a co s nimi před výsledným předáním provede.

3.4.7 Služba zabezpečení Active Directory

Active Directory je adresářová služba ukládající informace o objektech v síti a jejich vzájemných vztazích, umožňuje správcům sítě ale i uživatelům nastavovat politiku zabezpečení k aplikačním a datovým zdrojům. Primárním úkolem je poskytování centrálních služeb pro autorizaci a autentizaci uživatelů v síti a spravování uživatelských účtů. Dále umožňuje spravovat politiky jednotlivých počítačů, tedy co je na nich povoleno a co zakázáno spouštět či instalovat. Active Directory je založena na standardních internetových protokolech, jednoznačně a jasně definuje struktury sítě a organizuje skupiny počítačů.

3.4.8 Sumarizace použití

Pro informační systém podpory krizového řízení Policie ČR budou použity HTML dokumenty s podporou dynamického zpracování ASP stránek na straně webového serveru. Pro ukládání a manipulaci s daty bude použita SQL relační databáze s podporou SQL dotazů do databází. Vytvořené HTML stránky budou následně prostřednictvím protokolu HTTP(S) distribuovány uživatelům po vnitřní policejní intranetové síti. Bude využito stávajícího technického vybavení jak na straně serverů, tak na straně uživatelů. Pro identifikaci uživatelů v informačním systému bude využito doménového přihlášení Active Directory, které již bylo v rámci Policie ČR nasazeno a je využíváno.

To vše spolu s uvedenými technologiemi je v souladu s prvotním požadavkem na nulové investice.

II. PRAKTICKÁ ČÁST

4 POPIS PROVEDENÍ

Praktická část sestává z několika částí, od popisu aplikací přímo souvisejících s podporou krizového řízení, popisem aplikací návazných na základní systémy a rozšiřujících možnosti získávání informací, zabezpečení přístupu k neveřejným informacím, až k instalaci vlastních aplikací jak na straně webové části, tak na straně části datové.

Informační systém pro podporu krizového řízení byl koncipován jako webová aplikace pracující na protokolu HTTP(S) s využitím dynamického zpracování jak na straně klienta (HTML, JavaScript, CSS), tak na straně serveru (ASP) s využitím databázového rozhraní SQL. Všechny HTML dokumenty byly optimalizovány pro webový prohlížeč Internet Explorer verze 6 a vyšší.

4.1 Grafická část

Jelikož se jedná o informační systém a ne o prezentační webové stránky byla grafická stránka aplikací zvolena spíše umírněnější. Celkový jednotný vzhled byl konzultován s policejním psychologem. Každé stránce dominuje jednotné záhlaví s globální a lokální nabídkou formou jednoduchých tlačítek. Specifické ovládací prvky jsou umístěny hned u daných prvků, aby se zamezilo přílišnému rolování stránky, případně hledání daného ovládacího prvku. Vše je laděno do odstínu modré, které je dominující barvou Policie ČR a působí nerušivým dojmem i při dlouhodobé pracovní činnosti. Pouze důležitá informační sdělení či upozornění na kritické části při práci jsou výrazně barevně odlišeny a to především červeným textem. Většina datových výstupů je řazena dle předem stanoveného pořadí, případně dle abecedy nebo čísla, a často s možností vlastního setřídění.

Všechny aplikace byly optimalizovány pro dnes u policie standardní rozlišení 1024x768 s barevnou hloubkou True Color 32 bitů.

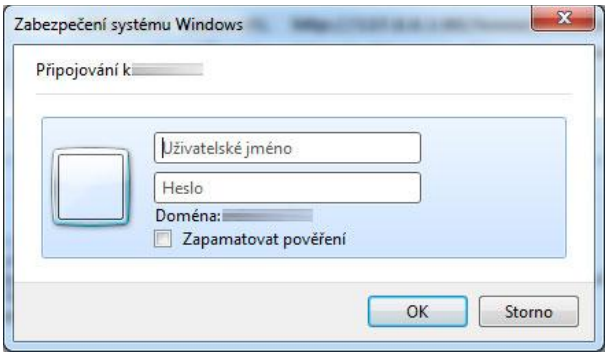
4.2 Adresářové rozmístění

Všechny aplikace jsou umístěny v jednom základním adresáři. V tomto adresáři se nachází také všechny globální soubory a soubory nastavení, které jsou využívány všemi ostatními aplikacemi. Například je zde uložen šifrovaný soubor s konekt stringem, ve které je uložena informace potřebná pro provázání webových aplikací na databáze, nebo soubor s globálním popisem kaskádových stylů CSS. Výhodou tohoto uspořádání je jednotnost pro všechny aplikace, kdy například v případě přesunu celého souboru aplikací na jiný webový server stačí změnit cesty potřebné pro činnost jednotlivých aplikací na jediném místě bez nutnosti zdlouhavého editování jednotlivých aplikací. Obdobně při přesunu databází na jiný SQL server stačí změnit konekt string na jediném místě. Každá samostatná aplikace je navíc umístěna ve vlastním adresáři i se svým vlastním specifickým nastavením. Tím je dosaženo vzájemného nenarušování jednotlivých aplikací mezi sebou. Souhrnně řečeno, každá aplikace má svůj vlastní prostor obsahující jen její soubory a nastavení a všechny dohromady využívají globální soubory a nastavení nacházející se v prostoru nad jednotlivými aplikacemi.

4.3 Doménové a aplikační zabezpečení

Pro přístup do jednotlivých aplikací se musí uživatel přihlásit do policejní domény. Tato povinnost je ve valné většině zajištěna umístěním jednotlivých policejních počítačů do domény, kdy uživatel se do domény přihlašuje již vlastním přihlášením do počítače. U výpočetní techniky, která není v doméně umístěna, je uživateli při přístupu zobrazeno přihlašovací okno s požadavkem vložení přihlašovacího jména a hesla. Všechny aplikace ASP skriptem *request.servervariables("LOGON_USER")* snadno zjistí přihlašovaný účet a podle toho nadále koordinují přístupy v rámci jednotlivých informačních systémů či jeho částí, případně neumožní uživateli přístup do těch částí aplikací, kam byl uživateli přístup buď zakázán, nebo nepovolen. Přístup do jednotlivých částí informačních systémů je pak řízen již aplikačně, kdy práva přístupu po ztotožnění uživatele jsou nalezena, nebo ne, v databázích a jednotlivé aplikace tak umožní, nebo ne, přístup přihlášenému uživateli. Varianta přihlášení se do domény a následné zpřístupnění již na základě informací uložených v databázích je výhodná z hlediska administrace zabezpečení Active Directory, kdy se nemusí pro každou změnu v přístupu do jednotlivých aplikací žádat administrátor domény o provedení změn. Souhrnně řečeno, uživatel se přihlásí svým doménovým účtem,

aplikace jej dle tohoto přihlášení ztotožní a nadále si již sami řídí přístupy do svých zabezpečených neveřejných částí.



Obrázek 1: Přihlašovací dialog

4.4 Programování na straně klienta – HTML, JavaScript, CSS

Při vytváření jednotlivých stránek informačního systému byl brán ohled na snadnou manipulaci, intuitivní ovládání, jednotný vzhled, tady celkově na user friendly. Všechny ovládací prvky interaktivně komunikují s uživateli změnou pozadí, bublinkovou nápovědou nebo informačními hláškami. Důvodem je, aby uživatel viděl, že aplikace funguje a reaguje na jeho pokyny, a aby v případě, kdy je počítač či server zaneprázdněn výkonem nějaké činnosti, neměl uživatel dojem, že mu zamrzl počítač. Potenciálně nebezpečné nebo nevratné operace jsou uživateli předem oznámeny s opakovaným požadavkem, chce-li v operaci pokračovat. Tímto je omezena riziková funkcionalita, kdy uživatel se mohl splést. Navíc všechna nebezpečná tlačítka, například mazání, jsou odlišena červeným pozadím.

Vkládací pole jsou, tam kde bylo zapotřebí, před vlastním odesláním údajů na server kontrolována na obsah, aby se zamezilo odeslání špatných dat a tím pádem zbytečnému vytěžování serveru. Například tam, kde je požadováno číslo, je před vlastním odesláním na server provedena kontrola obsahu vkládacího pole, je-li tam opravdu vloženo číslo, případně je-li v požadovaném rozsahu. Pokud je obsah vkládacího pole v pořádku, je údaj odeslán k dalšímu zpracování, pokud v pořádku není, stránka reaguje chybovou hláškou s popisem chyby, údaj na server odeslán není a po uživateli je požadována oprava.

Souhrnně řečeno, klientské stránky jsou vybudovány tak, aby se uživateli s nimi dobře pracovalo, aby se orientoval i bez hlubší znalosti daného informačního systému a aby měl pocit, že s ním aplikace spolupracuje.

4.5 Programování na straně serveru – ASP

Všechny ASP stránky v prvopočátku ztotožní přihlášeného uživatele a poté v případě neveřejných částí aplikací provedou dotaz do databáze na přístupové oprávnění daného uživatele. V případě existence platného přístupu je uživateli zobrazen obsah stránky, v případě opačném je stránka přesměrována na chybovou stránku s informací o neoprávněném přístupu. Protože tato procedura je na každé zabezpečené stránce, eliminuje se tak riziko neoprávněného přístupu a to i v průběhu vlastní práce.

Všechny údaje předávané serveru prostřednictvím metod GET nebo POST jsou validovány v přebírající ASP stránce, bez ohledu na skutečnost, že prvotní validace proběhla u klienta v jeho HTML stránce. Důvodem je, že validace u klienta je znalým uživatelem vyřaditelná, kdežto validace na straně serveru bez přístupu k serveru uživatelem proveditelná není. Ověření správnosti údaje u klienta slouží pouze pro omezení síťové komunikace mezi klientem a serverem, kdy drtivá většina špatných údajů je zachycena na počítači uživatele a nezatěžuje se tím síť a server. Přesto je každý údaj přijatý ASP stránkou na serveru znovu zkontrolován a teprve server rozhodne, je-li údaj správný a tedy bude dále zpracován, nebo je údaj chybný a bude klientovi vrácen. Tímto je potlačena chybovost při ukládání dat do databáze, kdy například textovou položku bychom se snažili vložit do číselného pole v databázi.

Emaily odesílané prostřednictvím ASP stránek jsou generovány za využití vestavěné komponenty *CDO.dll* jež je součástí operačního systému IIS serveru. Není tedy nutná instalace jakéhokoliv doplňujícího software. Příklad odeslání emailové zprávy z ASP stránky prostřednictvím CDO.dll komponenty:

set EMAIL=CreateObject("CDO.Message") – inicializace komponenty

EMAIL.from=odesilatel

EMAIL.to=příjemnce

EMAIL.cc=kopie

EMAIL.subject=předmět

EMAIL.textbody=tělo emailu

EMAIL.Send – vlastní odeslání

set EMAIL =nothing – uvolnění z paměti

Některé ASP stránky uložené na ostrém IIS serveru jsou kódovány funkcí ScrEnc, která ASP skript zakóduje do nečitelné, ale proveditelné podoby.

4.6 Programování na straně databáze – T-SQL

Všechny dotazy a požadavky do databáze jsou tvořeny uloženými funkce nebo uloženými procedurami. Rozdíl mezi nimi je v tom, že uložená funkce umožňuje data pouze vytěžovat, tak uložená procedura umožňuje data editovat. Z tohoto důvodu, jsou funkce používány tam, kde chceme data pouze získat a zobrazit, procedury se využívají tam, kde je požadavek na vytvoření, editaci nebo mazání dat. Veškeré potřebné údaje jsou funkcím a procedurám předávány formou parametrů, čímž je eliminována možnost editace SQL dotazu v ASP stránce. Jak funkce, tak procedury, jsou koncipovány na vrácení jen požadovaného množství informací, bez dalších údajů, což má za následek zvýšení výkonu a rychlosti výstupů. Všechny funkce a procedury jsou na ostrém serveru uloženy v šifrované podobě, čímž se eliminuje neoprávněná manipulace s obsahem daného SQL skriptu.

Příklad vytvoření šifrované uložené funkce nebo procedury:

CREATE FUNCTION název	*CREATE PROCEDURE název*
WITH ENCRYPTION	*WITH ENCRYPTION*
AS	*AS*
...	...

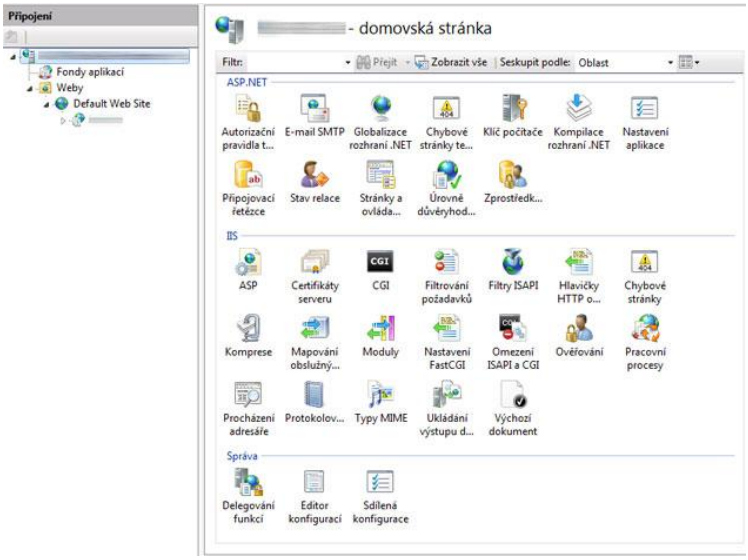
Nevýhodou šifrování je nemožnost zpětného dešifrování obsahu. Proto je nutné mít na zabezpečeném místě nešifrovanou podobu funkce nebo procedury pro případnou editaci.

4.7 Nastavení IIS serveru

Pro správnou funkcionalitu a zabezpečení je zapotřebí na webovém IIS serveru upravit konfigurační nastavení. Hlavní adresář obsahující globální soubory a v podadresářích jednotlivé aplikace je potřeba převést na pojmenovanou aplikaci. Tím se odstraní potřeba

uvádění plné cesty v adresářové struktuře webového prostoru a postačí jen uvedení názvu webového serveru spolu s názvem virtuální aplikace, aby byly nalezeny odpovídající spouštěcí ASP stránky. V nabídce „*ASP*“ se nastaví v položce „*Povolit nadřazené cesty*“ hodnota „*True*“, čím budou mít možnost jednotlivé podřízené aplikace využívat globální konfigurační a skriptové soubory. Dále v téže nabídce v položce „*Odeslat chyby prohlížeči*“ se nastaví „*False*“, čímž se v případě chybového stavu zamezí odeslání chybového hlášení klientskému počítači. V nabídce „*Výchozí dokument*“ se nastaví jako vstupní ASP stránka „*default.asp*“ čímž se potlačí spouštění ASP skriptů jiným než standardním způsobem. Posledním nastavením je v nabídce „*Ověřování*“, kde všechny položky budou nastaveny na „*Zakázáno*“, pouze položka „*Ověřování systému Windows*“ bude nastaveno na hodnotu „*Povoleno*“. Tím se zabrání anonymnímu prohlížení webového obsahu celého informačního systému a správa přístupů bude přesunuta na Active Directory.

Všechna uváděná nastavení postačí provést pouze na nejvyšším hlavním adresáři, protože veškerá nastavení se promítnou i do podřízených nastavení jednotlivých adresářů. Tím se usnadní celá správa webového prostoru pro případné další aplikace podléhající globálnímu nastavení. Dalším kladem je konfigurace na jediném místě, bez nutnosti opakujícího se nastavení pro podřízené aplikace.



Obrázek 2: Správa IIS

5 ZÁKLADNÍ ROZDĚLENÍ APLIKACÍ PRO PODPORU KRIZOVÉHO ŘÍZENÍ

Informační systémy používané v rámci činností Policie ČR a ministerstva vnitra jsou často vyvíjeny vlastními silami jednotlivých rezortů. Důvodů je několik, od vysoce specifických požadavků kladených na práci a manipulaci s policejními informacemi, až po zabezpečení dat nebo jejich přenosů. Informační systémy vznikají dle požadavků jednotlivých složek Policie ČR a jsou výsledkem časem prověřených postupů převedených do elektronické podoby. Mnoho aplikací vyvíjených pro potřeby Policie ČR nemá v komerčním sektoru mimo rezort obdobu. Dalším důvodem je bezpečnost, kdy není potřeba před civilními komerčními firmami zabývajícími se vytvářením softwarových produktů, rozkrývat strukturu postupů a zpracovávaných dat, čímž se minimalizuje nebezpečí úniku pracovních činností Policie ČR před neodpovědnými osobami.

Informační systém pro podporu krizového řízení a operačních středisek využívá některé globální aplikace a to „Organizační strukturu“ a „Databázi uživatelů“. Tímto způsobem není nutné potřebné informace nacházející se již v policejních databázích duplikovat, tedy existující informace budou použity pro potřeby informačního systému a budou přidány pouze informace, které jsou potřeba. Výhodou tohoto řešení je minimalizace zásahu do činností prováděných uživateli v již existujících informačních systémech tak, jak jsou zvyklí. Všechny aplikace mají jednotný grafický formát a jednotné ovládání, což z pohledu uživatele snižuje nároky na administrování nebo vytěžování. Často jsou používány číselníky, čímž je uživatelům usnadněna práce, kdy namísto vytváření specifických dat a tím pádem i rizik nejednotnosti je uživateli nabídnuta pouze možnost výběru z již existujících informací. Například v případě hodnostního označení „*poručík*“ by uživatelé mohli jeden a tentýž údaj zapsat mnoha způsoby „*Poručík, por., Por.*“, což by mělo v tomto případě za následek nechtěnou variabilitu a tedy nejednotnost, použitím číselníku s pouhou možností výběru se tohoto rizika vyvarujeme.

5.1 Organizační struktura

Organizační struktura je jedním ze základních informačních systémů Policie ČR umožňující, za využití předem definovaných typů strukturních objektů a v rámci nich vytvořených vztahů nadřízenosti a podřízenosti, sestrojit komunikační trasu, která odpovídá reálnému rozdělení funkčních kompetencí v rámci útvarů nebo jejich dílčích částí. Na takto definované komunikační trase je poté možné provozovat aplikace, které ke své činnosti využívají vytvořených vztahů „*nadřízený – podřízený*“ (například: telefonní seznam, distribuce dokumentů, distribuce oprávnění, plán vyrozumění, a další). Pro správné fungování návazných aplikací je nutné mít strukturu vytvořenu a spravovánu.

5.1.1 Vztahy mezi objekty struktury

Definování vztahu nadřízenosti a podřízenosti se provede tak, že pod výchozí (vstupní) bod struktury jsou postupně vkládány další a další podřízené a jim podřízené objekty. Následkem takto vytvořených a definovaných vztahů má každý objekt jednoznačně a přesně stanovené postavení ve struktuře a je mu určen právě jeden přímo nadřízený objekt. Samotný objekt může být zároveň nadřízeným více jiným objektům. Vztah nadřízenosti a podřízenosti je důsledně dodržován a umístění objektu na struktuře odpovídá i množství podřízených objektů. Platí, že objekt na struktuře výše postavený je nadřízený všem objektům níže postaveným v dílčích částech struktury. Praktické uplatňování této podmínky je prováděno dynamicky, a tak se všechny případné změny automaticky promítnou do struktury, do všech následných a souvisejících výpisů a do všech návazných aplikací.

Struktura je (v rámci informačních systémů provozovaných u Policie ČR) globálním systémem, jehož správu zabezpečují administrátoři (proškolení uživatelé), kterým je umožněn přístup do předem definovaných příslušných dílčích částí struktury.

Jednotlivé typy objektů předdefinovaných na struktuře jsou útvar, organizační článek, funkce a pracoviště.

Objekt typu útvar reprezentuje ve struktuře Prezidium a útvary, které byly ministrem vnitra v příslušném interním aktu řízení označeny za útvary s územní působností. V současné době se jedná o jednotlivá krajská ředitelství a útvary s celorepublikovou působností (např. Útvar pro odhalování organizovaného zločinu, Útvar rychlého nasazení, Pyrotechnická služba, a mnoho dalších).

Objekt typu organizační článek ve struktuře obvykle označuje organizační článek útvaru či nižší organizační článek podřízené struktury (odbory, skupiny, oddělení, a další).

Objekt typu funkce reprezentuje ve struktuře funkci zařazení. Prostřednictvím tohoto typu objektu se organizační struktura provazuje s databází uživatelů, tedy uživatelé nejsou přímo součástí struktury, ale jsou přiřazováni na existující objekty (funkce).

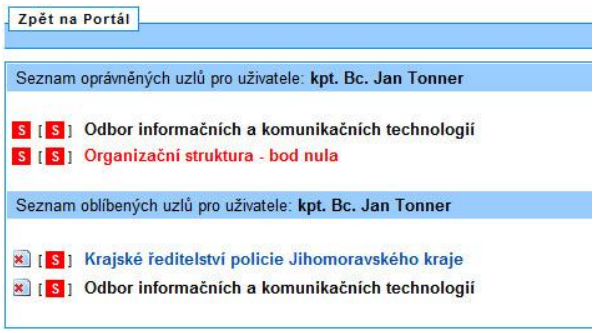
Objekt typu pracoviště není zcela plnohodnotným objektem struktury, slouží zejména pro zaznamenání kolektivních kontaktních údajů (například: učebna, vrátnice) tam, kde není možné nebo žádoucí jednoznačně přiřadit údaje k uživateli.

Toto řešení, kdy organizační struktura není tvořena uživateli, ale funkcemi, na které jsou následně uživatelé přiřazováni, má nespornou výhodu ve využívání struktury jinými informačními systémy. Lze tak definovat požadavky na pracovní činnost ne uživateli, ale funkci. Jinou pracovní náplň má kriminalista, jinou pracovník materiálně technického zabezpečení, jinou řidič a jinou pracovník ostrahy. Každá funkce sebou nese svou vlastní skladbu povinností, odpovědností, či jinou množinu údajů či dokumentů potřebnou k výkonu pracovní činnosti. Pro příklad uveďme povinnost seznamování se s dokumenty vydávanými nadřízenými složkami. Ředitel územního celku má za povinnost seznamovat se s dokumenty typu rozpočtu pro jím spravovaný útvar, různé statistické výstupy výslednosti, či smlouvy uzavřené mezi daným útvarem a mimorezortními firmami. Zaměstnanec skupiny informační podpory má jinou skladbu povinností, například zabezpečení výpočetní techniky antivirovými programy, zálohování databází či instalací potřebného software na policejní techniku. Každá z těchto dvou v příkladu uvedených funkcí sebou nese jinou pracovní činnost, jiný počet a typ informací a jiné povinnosti. Tedy ředitel nebude řešit instalaci programů a programátor nebude řešit podpis smlouvy na výměnu oken s firmou XY. Pokud z jakéhokoliv důvodu dojde k výměně zaměstnance na dané pozici, díky organizační struktuře není potřeba složitě řešit přidělování práv pro přístup k návazným informačním systémům, skladbu předpisů či jiných dokumentů potřebných pro výkon funkce a jiná nastavení. Stačí jen usadit uživatele na v rámci organizační struktury vytvořenou funkci a uživatel automaticky převezme všechny povinnosti uložené funkci.

5.1.2 Administrace organizační struktury

Administrátoři organizační struktury spravují dílčí části struktury (uzly), které jsou podřízeny objektům, na které mají přidělena některé z administrátorských oprávnění. Práv administrace jsou čtyři druhy. Nejnižší oprávnění [E] umožňuje spravovat organizační strukturu, tuto provazovat s jednotlivými uživateli z databáze uživatelů a dále spravovat základní údaje těchto přiřazených uživatelů. Vyšší oprávnění [N] navíc umožňuje vytvářet nové uživatele v databázi uživatelů. Druhé nejvyšší oprávnění [M] umožňuje mimo již zde uvedené kompletní správu uživatelů, tedy uživatele vytvářet ale i mazat. Nejvyšší oprávnění [S] navíc dovoluje editovat doménové údaje u jednotlivých uživatelů přiřazených na struktuře v rámci podřízené organizační struktury.

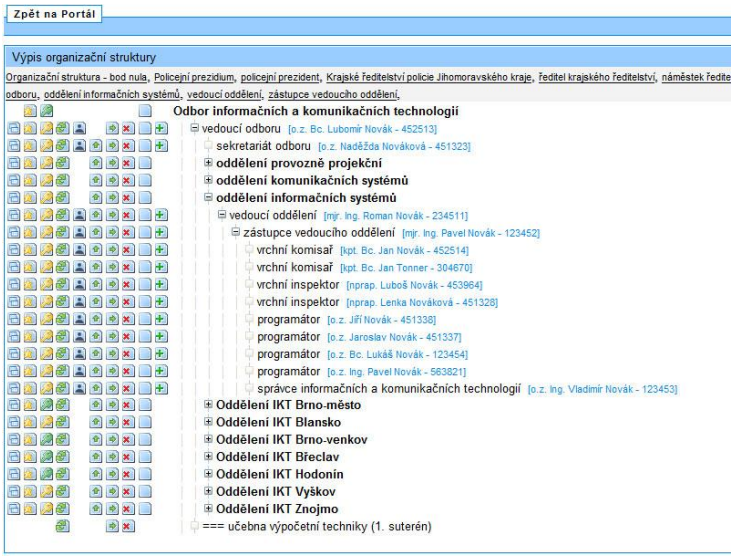
Jeden administrátor může spravovat více částí organizační struktury. Seznam oprávněných administrovaných uzlů se uživateli zobrazí na vstupní obrazovce do aplikace, kde jednotlivé položky seznamu jsou odkazy na příslušné přidělené uzly s označením typu oprávnění administrace. Dále si může administrátor v průběhu své práce definovat oblíbené uzly, které se poté zobrazí v základní nabídce a umožní mu rychlejší a komfortnější pohyb po rozsáhlých strukturách jím spravované oblasti. Díky tomu se nemusí zdlouhavě proklikávat od počátečního uzlu k uzlům hluboko zanořeným v organizační struktuře a často spravované oblasti si tak označí a poté najde mnohem rychleji.



Obrázek 3: Seznam uzlů

Administrátor si výběrem požadovaného uzlu zobrazí (rozbalí) podřízenou organizační strukturu a je mu umožněno s ní pracovat dle přiděleného oprávnění. Administrátorovi je umožněno přidávat nové podřízené objekty, měnit typy, názvy, zkratky a stavy již přidaného objektu, přesunovat objekty, definovat pořadí objektů v rámci úrovně, vkládat,

editovat či mazat kontaktní údaje, určovat administrátory podřízených uzlů, mazat objekty, přiřazovat uživatele na funkce a vkládat nebo měnit údaje uživatelů přiřazených na podřízených funkcích. Tlačítka pro provedení těchto činností jsou administrátorovi dostupná v levé části základního výpisu ze struktury ikonkami. Každý z rozličných typů objektů na struktuře má vlastní sadu těchto ikonek umožňující rychle vykonat potřebnou operaci s objektem nebo vede k otevření dialogového okna s dalšími možnostmi pro správu daného objektu.



Obrázek 4: Výpis spravované struktury

Výběrem požadovaného objektu nebo uživatele se administrátor dostane do detailu daného objektu s možností editace jeho vlastností. Vedle základních údajů jako je název, typ objektu, viditelnost, aj., je zde umožněno spravovat kontaktní informace pro potřeby ostatních informačních systémů. Byť pro správu osobních údajů jednotlivých uživatelů slouží jiná aplikace, byla administrátorovi dána možnost editovat alespoň základní údaje jím spravovaných uživatelů, neboť ne všichni zaměstnanci Policie ČR mají z rozsahu svých pravomocí přístup k informačním systémům, byť je jich velmi omezená skupina (například pracovníci úklidu přístup nemají). Přesto jsou i tito zaměstnanci zavedeni do databáze, i když jen z toho důvodu, aby bylo v případě potřeby možné zjistit jejich kontaktní informace.

Obrázek 5: Detail objektu a uživatele

Organizační struktura umožňuje stanovit stav každého objektu na hodnotu viditelný nebo neviditelný. Důvodem této operace je skrytí některých částí struktury nebo uživatelů z veřejných výstupů a přístupu všech uživatelů k těmto informacím. K takto nezobrazeným údajům má přístup pouze určitá, předem definovaná, skupina lidí. Neviditelnost objektů má tři stupně úrovně. První úrovní je skrytí uživatelů [N], kdy organizační struktura je zobrazena ale neviditelní uživatelé se ve výpise jeví, jako neobsazená funkce, tedy funkce neprovázaná s databází uživatelů. Druhou úrovní je skrytí objektu struktury [N], kdy se neviditelný objekt nezobrazí ve výpise i s uživatelem na tomto objektu (funkci) přiřazenému. Poslední třetí úrovní je neviditelnost zděděná pro objekty na struktuře [N], které jsou podřízeny objektu, na který byla přímá neviditelnost uplatněna.

Obrázek 6: Značení neviditelnosti objektů struktury

Skrytí určitých částí organizační struktury nemá za následek omezení činností v informačních systémech uživatelů podléhajících zneviditelnění. Jde jen o omezení průchodu informací do veřejně přístupných výstupů, kde by mohlo dojít ke zneužití těchto dat ať úmyslného či neúmyslného. Zaměstnanci speciálních složek policie mají také své povinnosti a odpovědnosti, ale ostatní uživatelé informačních systémů by o jejich činnosti neměli mít žádné informace, nejlépe by ani neměli mít tušení, že existují. Standardním řešení v rámci organizační struktury je vytvoření viditelného speciálního útvaru, viditelného ředitele, který tomuto útvaru velí a je většinou mediálně znám a viditelného pracovníka sekretariátu, aby bylo možno s tímto útvarem komunikovat. Všichni ostatní zaměstnanci jsou zneviditelnění. Uživatel vně tohoto útvaru tedy dostane informaci o existenci tohoto speciálního útvaru a prostřednictvím kontaktních informací na sekretariát může s tímto útvarem komunikovat. Všechny ostatní informace o tomto útvaru jsou mu odepřeny, tedy nejsou mu zobrazeny.

5.1.3 Zabezpečení administrace organizační struktury

Pro přístup k činnostem v rámci organizační struktury je zapotřebí se doménově přihlásit. Po ověření uživatele přihlašovacím jménem a heslem si informační systém sám z databáze zjistí oprávnění daného uživatele a podle druhu tohoto oprávnění mu upraví jeho administrační nabídky. Uživatelům s nulovým oprávněním není umožněn vstup a informační systém na tuto skutečnost reaguje informačním oknem se zprávou o nemožnosti přístupu. Toto ověření přístupu se provádí na každé stránce, ne jen na úvodní, tedy aplikace si kontroluje práva přístupu v každé své části, a pokud i v průběhu práce daného administrátora dojde ke změnám v jeho přístupu (například zásahem nadřízeného administrátora) je tato změna okamžitě aplikována. Výhodou tohoto způsobu je minimalizace nebezpečí neoprávněného přístupu či pokusů o něj do struktury jako celku, nebo do jiných částí než povolených.

Administrátoři jsou k práci s organizační strukturou vyškoleni svými nadřízenými administrátory, kteří tím odpovídají za jejich činnosti v rámci správy struktury. Nyní organizační struktur spravuje cca 2000 administrátorů z celé Policie ČR. Při počtu zhruba 60 tisíc zaměstnanců je to na první pohled vysoké číslo, ale každý z administrátorů spravuje pouze malou omezenou část struktury a nese za ni odpovědnost. Je mnohem výhodnější spravovat jedno oddělení s několika desítkami maximálně stovkou objektů, než mít na starosti rozsáhlejší část s tisíci a více objekty. Menší množství je snáze spravovatelné a je zde menší pravděpodobnost výskytu chyb. Původní myšlenka byla nechat administraci organizační struktury na jednotlivých personálních odděleních, praxe ale ukázala, že toto řešení nebylo šťastné, neboť personální pracovníci neměli dostatečné informace pro rychlé změny struktury a správa tak byla pomalá a navíc zde byly tendence k vytvoření papírového formuláře, pomocí něhož by jednotlivé odbory žádali o změnu. Proto se přistoupilo k řešení nechat jednotlivé odbory, skupiny či jednotlivé územní celky, aby si svou strukturu spravovali sami a přizpůsobovali si ji podle svých potřeb. Administrace tedy byla přenesena na vedení těchto organizačních celků, kdy ve velké většině případů strukturu administruje vedoucí daného organizačního celku spolu se svým administrativním pracovníkem.

5.1.4 Praktické řešení administrace organizační struktury

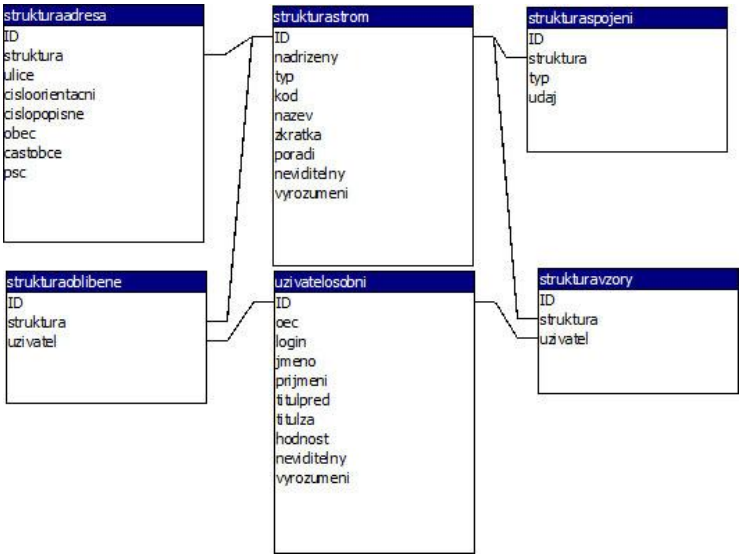
Organizační struktura je nevyvážený strom (hierarchie) obsahující jeden speciální kořenový objekt a jemu podřízených několik desítek tisíc objektů různých typů. Na kořenu struktury jsou přiřazeni čtyři superadministrátoři vidící celou strukturu s možností její správy. Úkolem superadministrátora není strukturu spravovat, ale pouze dohlížet. Tímto superadministrátorem byly vytvořeny jednotlivé kraje a celorepublikové útvary, poté byli sezváni schopní uživatelé těchto jednotlivých celků a byli vyškoleni na správu organizační struktury. Po jejich proškolení jim byly dány administrační oprávnění v potřebném rozsahu na jejich části struktury. Tedy superadministrátor vidí a může spravovat vše, podřízený administrátor se může pohybovat již jen v jemu přidělené části struktury a do jiných oblastí přístup nemá. Takto vyškolený administrátor si vytvoří základní strukturu daného kraje po jednotlivé odbory či územní celky a sezve si z těchto odborů schopné uživatele, proškolí je a přidělí jim správu dalšího již opět menšího celku. Tímto způsobem dojde k rozdrobení správy organizační struktury na malé snadno spravovatelné části, kdy vyšší administrátor kontroluje nižší administrátory a spravuje si svou malou část struktury. Pokud se vyskytne

problém a administrátor nemá možnost některé operace provést, například proto, že má potřebu sáhnout do části struktury, kam nemá oprávnění, kontaktuje s požadavkem nadřízeného administrátora.

Toto praktické řešení se ukázalo jako životaschopné, struktura je živá a využívaná jinými informačními systémy, ve kterých je potřeba pracovat s uživateli, což je dnes drtivá většina informačních systémů provozovaných u Policie ČR. Takto jsou všichni zaměstnanci Policie ČR soustředěni v jediné databázi a jakákoliv změna uživatele se nemusí provádět v mnoha jiných informačních systémem, ale jen a pouze na jednom jediném místě. Struktura se jako taková mění velmi málo, a když už tak pouze začátkem roku rozhodnutím politiků, kdy některé útvary vznikají nebo zanikají (například zrušením cizinecké policie, atd.)

5.1.5 Datová struktura organizační struktury

Organizační struktura je koncipována do třech základních a dvou pomocných relačních tabulek. První tabulka *strukturastrom* obsahuje hierarchické uspořádání jednotlivých objektů včetně základních údajů o objektu jako je název, typ, nadřízený objekt, určení viditelnosti či neviditelnosti, atd. Druhá tabulka *strukturaspojeni* obsahuje veškeré informace o služebních telefonech, mobilech, FAXech, emailových adresách, webových stránkách, …, které jsou vztaženy k jednotlivým objektům na struktuře. Jde především o informace z jednotných číselníkových plánů, vytvořených na pracovišti informační a komunikační podpory policejního prezidia. Třetí tabulka *strukturaadresa* obsahuje kontaktní adresy objektů, především útvarů či odloučených pracovišť. Pomocnými tabulkami jsou *strukturaoblibene* obsahující spravované uzly jednotlivých administrátorů pro rychlejší pohyb po rozsáhlé struktuře, a *strukturavzory* pro uložení aktuálního objektu, který může administrátor organizační struktury použít pro klonování objektů. Pomocné tabulky jsou propojeny s tabulkou uživatelů popsanou v kapitole o propojení organizační struktury s databází uživatelů.



Obrázek 7: ER diagram organizační struktury

5.2 Administrace osobních údajů

Druhým základním informačním systémem, který je zapotřebí pro provoz ostatních informačních systémů využívajících organizační strukturu je Administrace osobních údajů. Na rozdíl od organizační struktury, je administrace osobních údajů jednotlivých uživatelů z valné většiny ponechána na správě samotných uživatelů, kteří mají nařízením policejního prezidenta za povinnost si své osobní údaje udržovat v aktuální podobě. Vychází se z myšlenky, že nejlepší a nejaktuálnější informace o uživateli má uživatel samotný, a proto se odstranily různé formuláře, pomocí nichž žádal uživatel o správu svých dat oblastní administrátory, a uživateli je umožněno, tedy spíš nařízeno, se o své údaje starat sám. Tímto způsobem se výrazně zvýšila informační úroveň uložených dat. Data změněná uživateli se automaticky promítnou do všech návazných informačních systémů. Osobní údaje, které jsou uživateli zpřístupněny pro vlastní správu, může v omezené míře editovat i administrátor organizační struktury, byť toto není standardním řešením. V praxi existují uživatelé, kteří nemají přístup k vnitřní intranetové síti, či uživatelé dlouhodobě postavení mimo službu, ať už z důvodu nemoci či dlouhodobého pobytu v zahraničí. Proto administrátoři organizační struktury tuto možnost editace osobních údajů mají.

Uživatelé nejsou standardně součástí organizační struktury, ale jsou na ni navázáni prostřednictvím objektu typu funkce, kdy se uplatňuje pravidlo jeden uživatel je spojen s jednou funkcí. Není možné přiřadit uživatele na více funkcí, je však možné pomocí

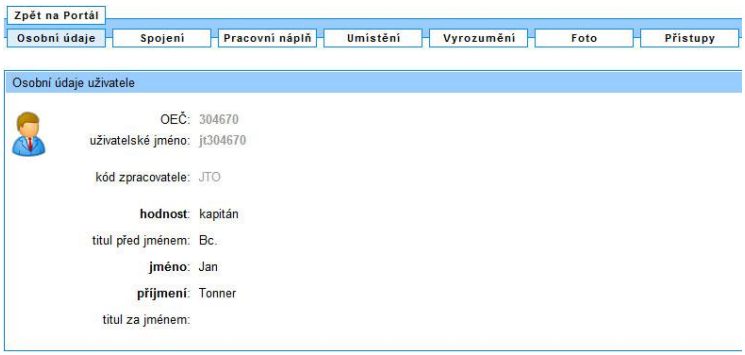
delegování oprávnění umožnit danému uživateli správu i jiných částí v rámci návazných informačních systémů. Přiřazení na strukturu provádí administrátor dané oblasti na základě pokynu příslušného nadřízeného a uživateli tímto vznikne takové postavení v organizační struktuře, na kterou je navázán. Zároveň s přiřazením převezme uživatel práva přístupů do informačních systémů, které jsou navázány na funkci z organizační struktury. Tímto způsobem je velmi usnadněna správa přístupů do různých informačních přístupů, není nutné uživateli přístupová oprávnění neustále editovat v případě pohybu uživatele po struktuře, jen se nadefinují oprávnění pro funkce, vyplývající ze zařazení, a usazením uživatele dojde k převzetí definovaných práv.

5.2.1 Vlastní administrace osobních dat

Veškeré údaje uložené o uživateli jsou rozčleněny do několika typově příbuzných množin dat. Až na pár výjimek, jsou tyto údaje součástí veřejných výstupů, o uživateli je možné zjistit z veřejných výstupů všechny potřebné informace. Uživateli je prostřednictvím vkládacích a výběrových polí umožněno udržovat aktuální podobu valné většiny informací, které jsou vedeny a uloženy k jeho sobě.

Jednotlivé sekce pro editaci osobních údajů:

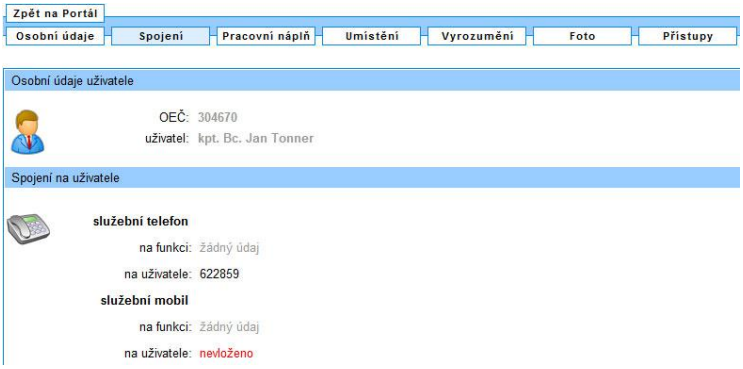
Osobní údaje – jméno a příjmení, hodnost, tituly jak před tak za jménem, kód zpracovatele, plus pro uživatele needitovatelné informace z domény, které může změnit jen administrátor organizační struktury s právem [S].



Obrázek 8: Osobní údaje

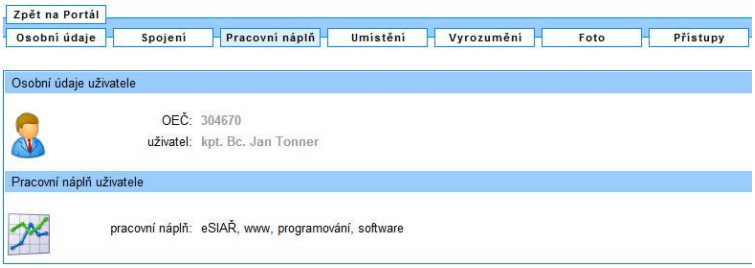
Spojení – služební telefon, služební mobilní telefon, služební FAX, služební emailová adresa a služební intranetové stránky. Slovo „služební“ je zde uvedeno a opakováno záměrně, aby si uživatel uvědomil, že zde nevyplňuje své osobní kontaktní informace, ale

služební, platné v rámci rezortu. Uživateli jsou zobrazeny i kontaktní informace vedené na přiřazené funkci, ale bez možnosti editace, kterou má právo provádět jen administrátor dané oblasti. Uživatel v případě nesrovnalostí může daného administrátora kontaktovat a nesrovnalost s ním konzultovat. Kontaktních informací může uživatel mít neomezené množství, je vhodné uvést i kontakty na místa, kde se uživatel často pohybuje.



Obrázek 9: Spojení

Pracovní náplň – tato položka je určena pro další doplňující informace k uživateli, využívá se pro základní policejní činnosti, například majetkový kompetent, předseda odborové organizace, atd. Tyto informace umožňují blíže specifikovat činnost uživatele, jsou součástí veřejných výstupů a napomáhají rychleji vyhledat kompetentní osobu pro řešení jakéhokoliv problému. Například uživatel potřebuje řešit nějaký problém s SQL databází, z veřejného výpisu z oddělení informační podpory dostane 10 - 15 pracovníků a z položky pracovní náplň vybere toho, kdo se problematikou SQL zabývá.



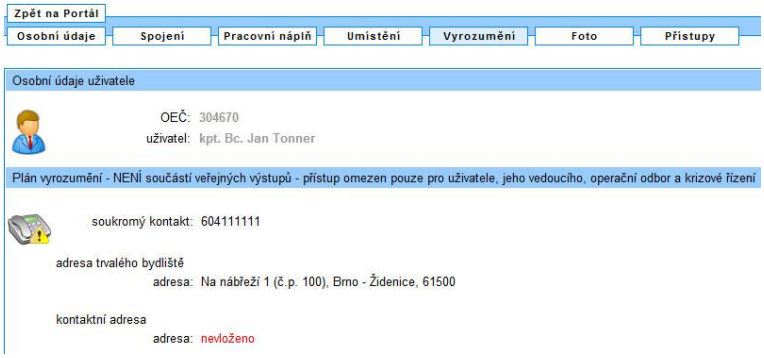
Obrázek 10: Pracovní náplň

Umístění – adresa pracoviště, číslo kanceláře, číslo intranetové zásuvky, ale i informace o umístění na organizační struktuře s kontaktem na nejbližšího oblastního administrátora, do jehož pravomoci daný uživatel spadá. Údaje o adrese pracoviště jsou pro uživatele pro

editaci nepřístupné, jsou zde pouze pro informaci, tyto údaje spravuje administrátor organizační struktury a jsou z valné většiny uvedeny pouze u útvaru a podřízené objekty je z tohoto nadřízeného objektu zdědí.

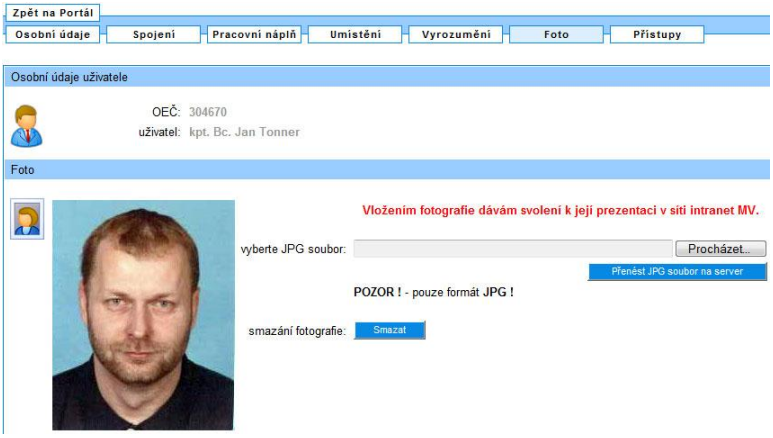
Obrázek 11: Umístění

Vyrozumění – soukromý kontakt, soukromá adresa uživatele, případně kontaktní adresa. Tato část slouží ke vložení kontaktních informací tak, aby bylo možné v případě nutnosti uživatele rychle kontaktovat a informovat o nenadálých skutečnostech, případně o urychleném přesunu na pracoviště. Všechny informace umístěné v této sekci nejsou součástí veřejných výstupů, přístup k nim mají pouze nadřízení daného uživatele, příslušné krizové pracoviště a příslušný operační odbor na což je uživatel upozorněn. Tyto údaje jsou kvalifikovány jako informace soukromého charakteru a jakýkoliv přístup k nim je logován a zpráva o jejich zobrazení je uživateli sdělena.



Obrázek 12: Vyrozumění

Foto – slouží k uložení fotografie uživatele. Není to povinná část, nicméně se doporučuje uživateli fotografii vložit. Ukládá se zde fotografie pořízená při nástupu uživatele k policii, kdy je každému uživateli vyhotovena rezortní identifikační karta, jíž je fotografie součástí. Fotografii do systému může vložit pouze uživatel sám, neexistuje možnost tuto operaci provést jiným způsobem. Tímto je eliminována možnost vložení fotografie bez vědomí uživatele a na možnost výskytu fotografie ve veřejných výstupech je uživatel zřetelně upozorněn. Fotografie je v systému uložena jako JPG soubor s automaticky vytvořeným a needitovatelým názvem bez přímé souvislosti k uživateli, propojení s uživatelem je řešeno databázovým přístupem.



Obrázek 13: Foto

Přístupy – výpis z logů, kdo a kdy si zobrazil soukromé kontaktní informace uživatele. Zde má uživatel možnost si zkontrolovat, kdo, kdy a pomocí jakého programu či informačního systému si zobrazil (požádal o) jeho soukromé informace. Tato část zároveň slouží jako prevence proti sice oprávněnému, ale bezdůvodnému prohlížení neveřejných informací a výstupy z logů se pravidelně kontrolují a výsledky se předávají generální inspekci ozbrojených složek, která na jejich základě prování kontrolní činnosti.

Obrázek 14: Přístupy

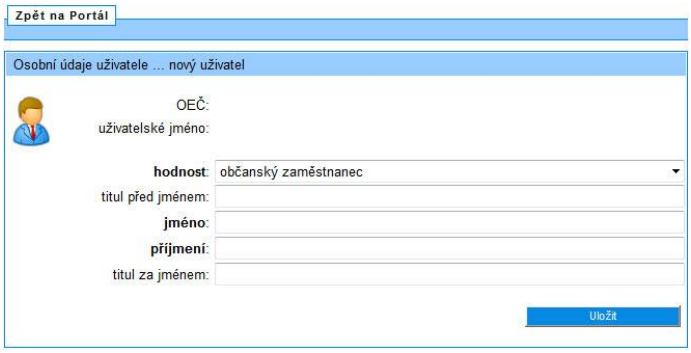
Až na sekci „*vyrozumění*“ a „*přístupy*“ jsou všechny údaje součástí veřejných výstupů a uživatel je na tuto skutečnost upozorněn. Dále je uživatel upozorněn, že za tyto údaje, jejich úplnost a pravdivost nese plnou odpovědnost on sám. Tímto způsobem je zabezpečeno, že uživatelé si sami hlídají své informace a v případě jejích neaktuálnosti si je sami změní, nebo v případě, kdy na editaci dat nemají práva, sami požádají příslušné administrátory k provedení nápravných kroků. Uživatelé, které administrátor organizační struktury označí jako neviditelné, se nebudou v žádných veřejných výpisech objevovat. Jejich údaje se zobrazí pouze oprávněných uživatelům. Veškerý přístup k těmto informacím je logován jak aplikačně tak i na úrovni operačního systému.

5.2.2 Zabezpečení administrace osobních údajů

Pro přístup k informacím v rámci administrace osobních údajů je zapotřebí se doménově přihlásit. Po ověření a ztotožnění uživatele přihlašovacím jménem a heslem jsou informačním systémem zobrazeny údaje přihlášeného uživatele. Toto ověření se provádí na každé stránce aplikace, ne jen na úvodní, tedy systém si kontroluje práva přístupu v každé své části. Výhodou tohoto způsobu je minimalizace nebezpečí neoprávněného přístupu či pokusů o něj.

5.2.3 Praktické řešení administrace organizační struktury nového uživatele

Po nástupu nového zaměstnance k rezortu ministerstva vnitra nebo Policie ČR je uživateli jako první vytvořen identifikační karta uživatele. Je jedno jedná-li se o služební poměr nebo o pracovně právní vztah, každý zaměstnanec Policie ČR identifikační kartu obdrží. Její součástí je identifikační číslo uživatele, které je jednoznačné (neduplicitní). Toto číslo je následně použito k vytvoření doménového účtu v policejní doméně vnitřní intranetové sítě. Následně je potřeba nového uživatele zavést do databáze osob, neboť z pohledu informačních systémů kdo není v databázi osob ten neexistuje. Nový uživatel se přihlásí svým účtem do administrace osobních údajů, aplikace ho nedokáže identifikovat, a proto mu vygeneruje přihlašovací formulář nového uživatele a požaduje jeho vyplnění. Vyplněním a uložením je uživatel zaveden do databáze osob a je mu nastaveno základní nastavení a základní přístupy do všech návazných informačních systémů.

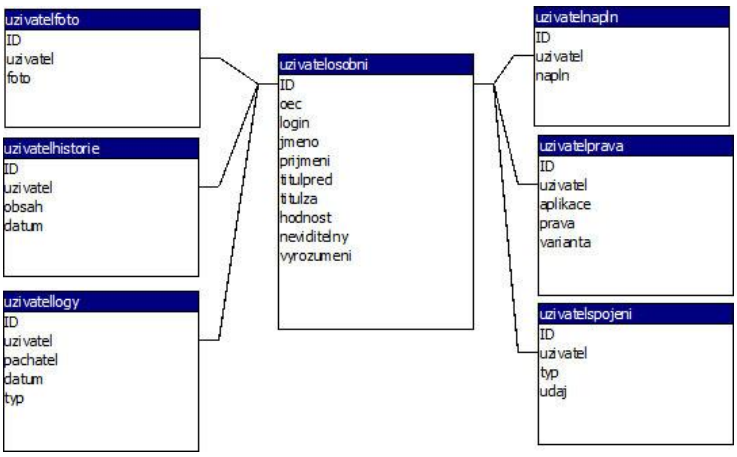


Obrázek 15: Nový uživatel

Následujícím krokem již existujícího, tedy známého uživatele, je vyplnění zbývajících osobních informací na základě pokynů či požadavků nadřízených orgánů.

5.2.4 Datová struktura databáze uživatelů

Databáze uživatelů je tvořena sedmi relačními tabulkami. Základní tabulkou je *uzivatelosobni* obsahující osobní údaje každého uživatele a to jméno, příjmení, tituly uváděné před a za jménem, osobní evidenční číslo, login v policejní doméně, určení viditelnosti či neviditelnosti, atd. Na tuto tabulku jsou navázány všechny ostatní tabulky a to *uzivatelfoto* obsahující název jpg obrázku uživatele, *uzivatelhistorie* obsahující změnové informace (například při změně příjmení je zde uvedeno kdy a kým došlo k editaci), *uzivatellogy* obsahuje informace o zobrazování dat soukromého charakteru jinými uživateli, *uzivatelnapln* obsahuje informace o pracovní náplni jednotlivých uživatelů, *uživatelprava* obsahuje přístupová oprávnění uživatelů do jednotlivých informačních systémů, pokud takové oprávnění bylo dáno přímou definicí, a poslední tabulka *uzivatelspojeni* obsahuje všechny informace o služebním a soukromém spojení na uživatele.



Obrázek 16: ER diagram databáze uživatelů

5.3 Propojení organizační struktury s databází uživatelů

Jak už bylo naznačeno v předchozím textu, organizační struktura a uživatelé jsou dvě rozdílné a do jisté míry na sobě nezávislé množiny dat. Pro správnou činnost návazných informačních systémů je potřeba tyto dvě množiny spojit do jednoho celku. Tuto činnost provede administrátor organizační struktury, kdy na objekt typu funkce přiřadí volného uživatele podle pravidla „*jedna funkce = jeden uživatel*“ a zároveň „*jeden uživatel = jedna funkce*“. Tím dojde ke sloučení informací vedených u objektu na struktuře s informacemi vedenými u daného uživatele. Tedy veškeré informace a nastavení z funkce přebírá uživatel a naopak veškeré informace a nastavení uživatele přebírá funkce. Například přiřazením uživatele „Jana Nováka“ na funkci „ředitele územního celku“ převezme uživatel právo přístupu do statistických informačních systémů či do přidělených dokumentů dané funkci, naopak funkce si z uživatele převezme kontaktní informace či uživatelské specializace. Toto propojení je zcela automatické a ve veřejných výstupech je barevně signalizováno, které údaje patří k objektům na organizační struktuře a které patří uživateli.

5.3.1 Základní seznam údajů vedených u objektu a uživatele

Každý objekt libovolného typu v organizační struktuře má tuto skladbu údajů:

- identifikační číslo objektu (jedinečné a neměnitelné),
- typ objektu (útvar, organizační článek, funkce, pracoviště),
- kód objektu (vychází z tabulkové systemizace Policie ČR),

- název objektu (vychází z tabulkové systemizace Policie ČR),
- zkratka objektu (vychází z tabulkové systemizace Policie ČR),
- stav objektu (viditelný, neviditelný),
- služební kontaktní informace (telefon, mobil, FAX, emailová adresa intranetová a internetová, www adresa intranetová a internetová),
- adresa objektu (korespondenční adresa).

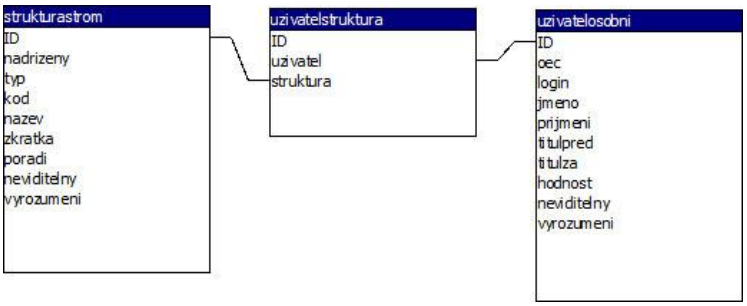
Každý uživatel má tuto skladbu informací:

- identifikační číslo uživatele (jedinečné a neměnitelné),
- osobní evidenční číslo (jedinečné číslo přidělené zaměstnanci při nástupu do rezortu, nemůže být duplicitní),
- login (v policejní doméně),
- hodnost,
- tituly před jménem,
- jméno,
- příjmení,
- tituly za jménem,
- kód zpracovatele,
- stav uživatele (viditelný, neviditelný),
- služební kontaktní informace (telefon, mobil, FAX, emailová adresa intranetová a internetová, www adresa intranetová a internetová),
- pracovní náplň,
- umístění (číslo kanceláře, číslo intranetové zásuvky),
- zaměření uživatele, specializace, metodika,
- vyrozumění v rámci plánu (kontaktní informace soukromého charakteru),
- fotografie.

Další informační systémy si tuto základní skladku údajů dále rozšiřují o potřebné informace v rámci toho kterého systému, například o informaci držení řidičského oprávnění a jeho variant, či o pořadí vyrozumění z plánu vyrozumění. Základní údaje vedené u objektů nebo uživatelů jsou tedy využívány všemi návaznými informačními systémy, specifické informace potřebné pro činnost jiných aplikací se administrují již v rámci těchto aplikací.

5.3.2 Datová struktura propojení organizační struktury s databází uživatelů

Datové propojení organizační struktury s databází uživatelů je provedeno za pomoci jedné relační tabulky *uzivatelstruktura* obsahující odkaz na základní tabulku organizační struktury *strukturastrom* a základní tabulku uživatelů *uzivatelosobni*. Každý záznam v těchto tabulkách má SQL databází automaticky vytvořeno vnitřní identifikační číslo (ID) identity(1,1), čímž je zajištěna referenční integrita mezi příslušnými záznamy. Vnitřní identifikační číslo nemohou uživatelé žádným způsobem měnit, mohou je pouze zjistit, a toto vnitřní identifikační číslo je platné a jednoznačné po celou bodu existence záznamu.



Obrázek 17: ER diagram propojení organizační struktury a databáze uživatelů

5.4 Plán vyrozumění

Při vyhlášení krizové nebo mimořádné události je jedním z prvotních úkolů operačního střediska informovat zainteresované osoby Policie ČR o této situaci dle pořadí vyrozumění. Ne každý zaměstnanec musí být informován okamžitě. Proto byly vytvořeny seznamy dle pořadí vyrozumění tak, aby zainteresované či odpovědné osoby byly vyrozumívány o vzniklé situaci v definovaných sledech a časových odstupech. Zamezí se tak nechtěnému chaosu a jednotlivé složky Policie ČR jsou aktivovány postupně jak v čase tak místě. V první fázi jsou informovány a povolány řídící struktury včetně hotovostních pracovníků, kteří po rozboru krizové nebo mimořádné situace aktivují další složky jak Policie ČR, tak i ve spolupráci s integrovaným záchranným systémem jiné záchranné či likvidační oddíly.

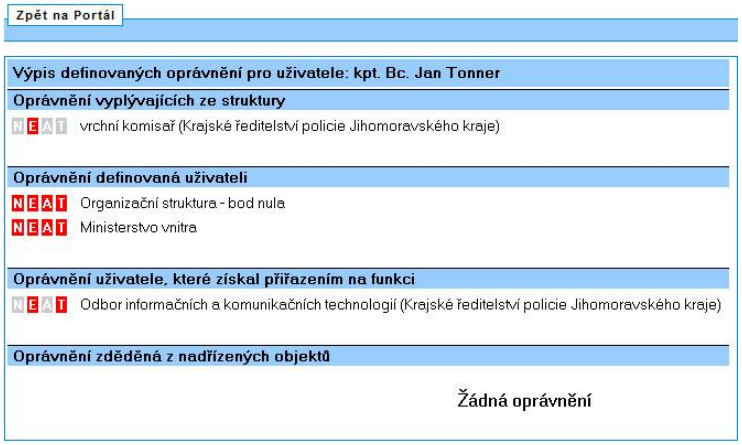
K těmto činnostem slouží informační systém „Plán vyrozumění“ umožňující předem definovat množiny zaměstnanců jak v rezortu tak mimo něj a držet kontaktní informace o těchto osobách.

5.4.1 Administrace plánu vyrozumění

Nejvyšším správce aplikace je superadministrátor, jehož jediným úkolem je definovat příslušné správce jednotlivých územních celků a přiřadit jim přístup do informačního systému. Jednotlivé územní celky jsou převzaty z organizační struktury včetně přiřazených uživatelů. Superadministrátor tedy vydefinuje přístupová oprávnění vyčleněným pracovníkům s definicí části organizační struktury, za kterou jednotliví správci přebírají odpovědnost. Tito správci mají za povinnost vytvořit na základě potřeb a požadavků skupiny zaměstnanců a rozdělit je dle pořadí vyrozumění.

Přístupová oprávnění může správce získat několika způsoby. Buď jsou mu přidělena nadřízeným administrátorem přímou definicí uživateli nebo obsazené funkci, nebo jsou zděděna z nadřízeného objektu, kterému správce podléhá. Při přímé definici jsou práva přístupu nepřenosná a slouží jen definovanému zaměstnanci. V případě oprávnění zděděného se právo přístupu uplatňuje na celou skupinu podřízených zaměstnanců. Důvodem je nemožnost přesného budoucího určení množiny správců, kteří budou tento informační systém využívat. Například operační středisko má v čase proměnlivou skladbu zaměstnanců, jedni přicházejí, jiní odcházejí, a bylo by tedy zapotřebí neustále upravovat přístupy jednotlivým zaměstnancům. Proto je mnohem výhodnější nastavit práva přístupu operačnímu odboru jako celku a všem podřízeným funkcím toto oprávnění nechat zdědit. Tak je v případě editace organizační struktury v tomto organizačním článku zajištěno, že i bez zásahu správce budou přístupová oprávnění automaticky neustále přizpůsobována aktuálnímu stavu tohoto odboru. Posledním způsobem získání přístupových oprávnění je vlastní přidělení na organizační struktuře. Jednotliví vedoucí pracovníci z titulu své funkce mají přístup do aplikace, byť jen velmi omezený. Mohou pouze prohlížet svou podřízenou část organizační struktury bez možnosti cokoliv měnit či definovat práva přístupu někomu jinému. Ale i tento omezený přístup jim umožňuje zjišťovat aktuální stav a tedy koordinovat činnosti jím řízeného organizačního článku dle zjištěných informací.

Po doménovém přihlášení a ztotožnění je jednotlivým správcům zobrazena úvodní obrazovka, kde najdou informace o přístupových právech a částech organizační struktury, kterou mají oprávnění spravovat.



Obrázek 18: Plán vyrozumění – seznam uzlů

Jednotlivá oprávnění jsou koncipována do čtyř základních skupin:

- [N] – právo na neviditelné objekty,
- [E] – právo na editaci skupin dle pořadí vyrozumění podřízeným strukturám,
- [A] – oprávnění definovat jiné podřízené administrátory (správce),
- [T] – oprávnění pro tiskové výstupy jak jednotlivých kontaktních seznamů, tak kontrolních seznamů.

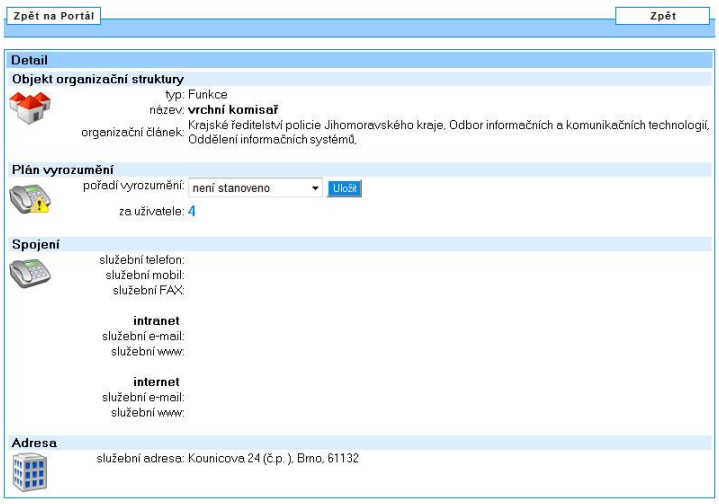
Správci s oprávněním [A] je umožněno vytvářet další administrátory v rámci své přidělené organizační struktury. Může přidělovat ta samá oprávnění, kterými sám disponuje, na celou jím spravovanou část organizační struktury. Tímto způsobem je možné rozdělit administraci rozsáhlých částí struktury do menších lépe upravovatelných podčástí a předat tak i odpovědnost za menší celky do správy jinému uživateli. Nadřízený správce pak přebírá již jen kontrolní případně poradní úlohu.

Obrázek 19: Definování nového správce

5.4.2 Editace skupin pořadí vyrozumění

Každý správce má za úkoly vytvářet skupiny pořadí vyrozumění. Jedná se o výběr pracovníků spravované organizační struktury a přiřazení pořadí, ve kterém budou vybraní pracovníci v případě vzniku krizové nebo mimořádné události vyrozumíváni. Standardně jsou využívány čtyři pořadí 1. až 4., kde dané číslo vyjadřuje prioritu. V případě potřeby jsou vyrozuměni zaměstnanci s pořadím 1. Ti jsou okamžitě dopraveni do krizového centra k rozboru a posouzení mimořádné situace a dle jejich pokynů se aktivují další pořadí pracovníků souběžně s krizovými plány.

Správce má při definování pořadí vyrozumění na výběr, zda bude pořadí přidělovat přímo uživateli, nebo funkci. V případě uživatele je pořadí přiřazeno přímo zaměstnanci bez ohledu na jeho umístění na organizační struktuře. Tato varianta se volí pro specialisty různých oborů a je pak bezpředmětné, jakou pozici zastávají. Ve druhém případě se definuje pořadí funkci bez ohledu na to, kdo ji zrovna zastává. Tato varianta je vhodná pro definování řídících struktur, například pořadí vyrozumění 1. je dáno veliteli útvaru, bez ohledu na to, který uživatel v danou chvíli tuto funkci vykonává. Vlastní editace je provedena v detailu uživatele nebo funkce.



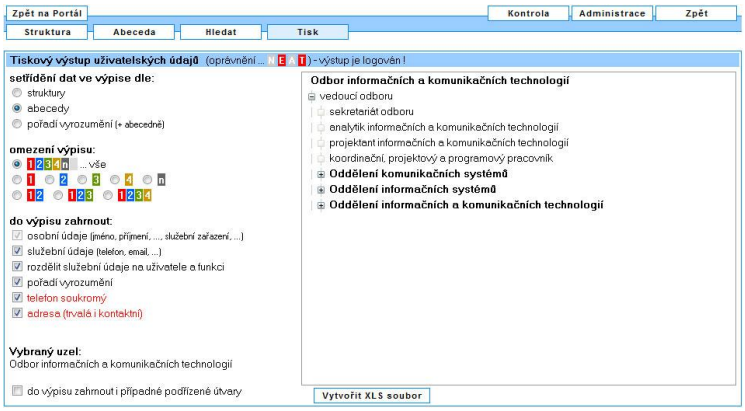
Obrázek 20: Editace pořadí vyrozumění

Přidělení pořadí vyrozumění se vztahuje pouze k uživateli nebo funkci. Vlastní skupiny takto vydefinovaných objektů jsou pak vytvářeny automaticky z umístění na organizační struktuře bez zásahu správce, standardně dle územních odborů. Tedy správci pouze vydefinují uživatele nebo funkce a přiřadí jim pořadí vyrozumění, a aplikace již pak sama

ve spolupráci s organizační strukturou vytvoří plány vyrozumění jednotlivých územních celků nebo útvarů s celorepublikovou působností.

5.4.3 Tiskové výstupy – plány a kontroly

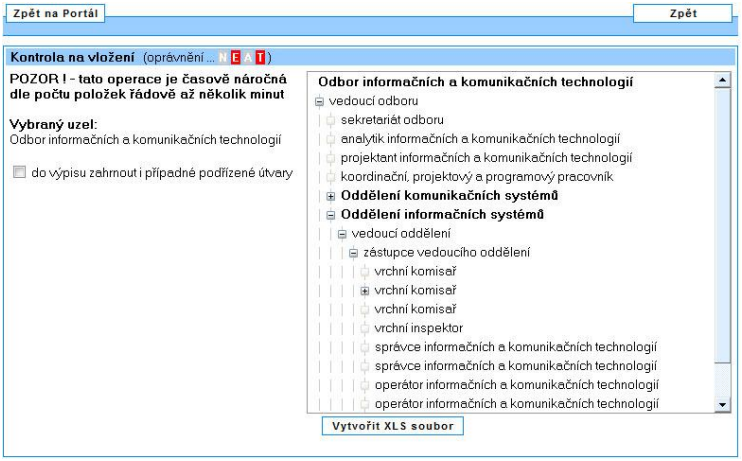
Byť je možné si jednotlivé plány vyrozumění zobrazovat elektronicky, je jedním z hlavních požadavků tiskový výstup, který se pravidelně, dle potřeb jednotlivých územních celků, aktualizuje a je v papírové podobě uložen na zabezpečeném místě na operačním středisku. Důvodem je nezávislost na elektrické energii, neboť v některých mimořádných situacích může dojít k jejímu výpadku. Například v případě rozsáhlých povodní mohou být dočasně odpojeny velké části přenosových sítí, přesto je zapotřebí svolat krizový štáb. Aplikace umožňuje správci s právem přístupu [T] tyto tiskové výstupy pořizovat. Jednoduchou formou je umožněno vydefinovat potřebné tiskové výstupy dle mnoha parametrů a třídění. Samotný výstup z aplikace je ve formátu *CSV*, který pak následně mohou jednotliví správci editovat v aplikaci Microsoft Excel. Důvodem je nejednotnost požadavků na tiskový výstup jednotlivými řediteli územních celků, a proto jsou poskytnuty v CSV souboru samotná požadovaná a setříděná data, a jak bude konečný výstup graficky vypadat, bylo ponecháno již na jednotlivých územních celcích.



Obrázek 21: Definování tiskového výstupu

Druhým tiskovým výstupem je výstup kontrolní, určený pro jednotlivé vedoucí pracovníky. Jak bylo uvedeno v administraci osobních údajů, veškeré informace o uživateli si řídí uživatel sám. Přesto je zapotřebí provádět kontrolu vedoucím pracovníkem, zda-li si jednotliví uživatelé tuto povinnost plní. Vedoucí pracovník má možnost zobrazit si detailní informace každého svého podřízeného pracovníka a kontrolu provést vizuálně. V případě velkého počtu podřízených je tato cesta neefektivní a zdlouhavá. Proto vedoucí pracovník

může požádat příslušného správce o kontrolní výstup jeho podřízených. Kontrolní výstup sestává z tabulky, kde jednotlivé řádky obsahují podřízené pracovníky a sloupce odpovídající kontrolované údaje. Vlastní údaje nejsou součástí kontrolního výstupu, je zde jen graficky výrazně indikováno, které údaje si podřízený pracovník do databáze nevložil. Na základě této informace pak vedoucí pracovník může provést následné kroky ke korekci tohoto stavu.



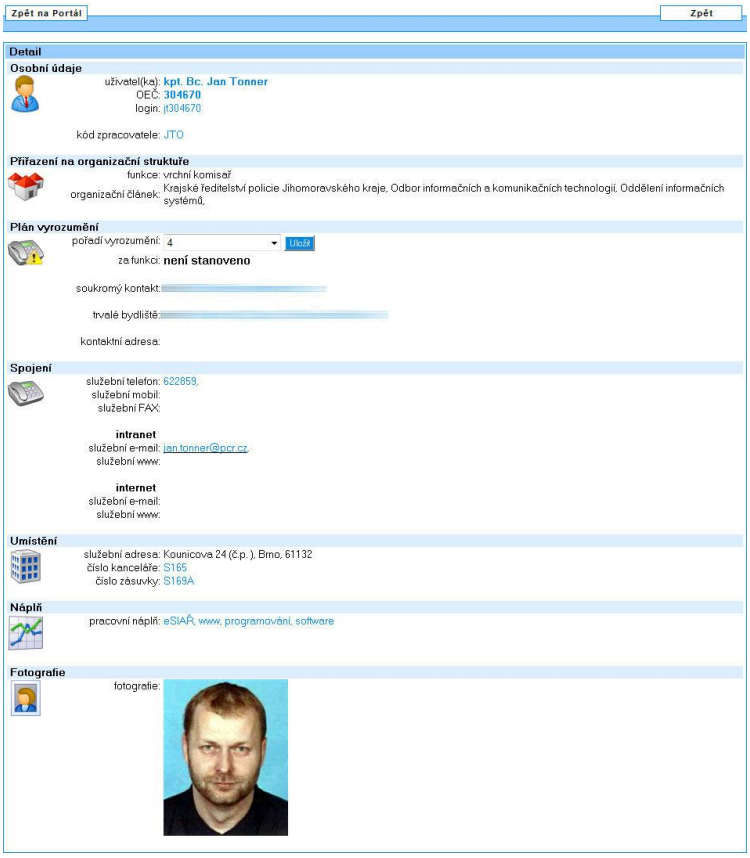
Obrázek 22: Definování kontrolního výstupu

5.4.4 Prohlížení – přístup vedoucího pracovníka

Z titulu své funkce je každému vedoucímu pracovníku umožněno nahlížet na podřízenou organizační strukturu, zjistit stav pořadí vyrozumění jednotlivých pracovníků a tím mít možnost koordinovat a řídit činnosti ve svém organizačním článku. Standardně je v plánu vyrozumění jednotlivým vedoucím odborů přiřazeno pořadí 1. nebo 2., podobně jako specialistům napříč celou organizační strukturou. Další zaměstnanci odborů jsou pak v pořadí zařazeni níže, neboť u mimořádných událostí jsou aktivováni krizovým štábem až v okamžiku potřeby nebo v okamžiku daném krizovým scénářem. Z výpisu své podřízené organizační struktury s uvedeným pořadím vyrozumění zjistí všechny potřebné informace, jednotlivé stupně pořadí, komu a jak byly přiděleny.

Obrázek 23: Výpis struktury vyrozumění

Výběrem funkce nebo uživatele je pak umožněno nahlédnou do detailu, tentokrát již s kompletními informacemi, tedy i s údaji soukromého charakteru. Toto zobrazení je uloženo do logů příslušných uživatelů, kteří tak mají možnost zjistit, kdo a kdy si tyto informace prohlížel, a do aplikačních logů pro případné kontroly generální inspekcí.



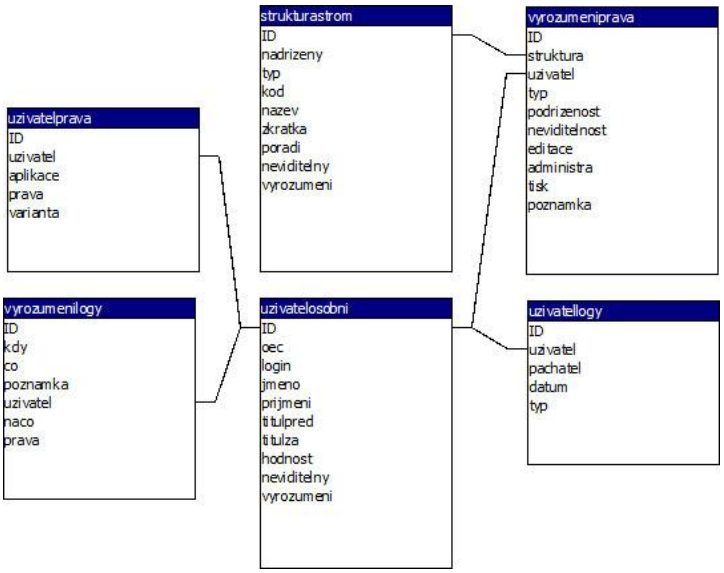
Obrázek 24: Detail uživatele v plánu vyrozumění

5.4.5 Zabezpečení plánu vyrozumění

Podobně jako u ostatních informačních systémů je i pro přístup do plánu vyrozumění potřeba se doménově přihlásit. Po ověření přihlašovacích informací a ztotožnění uživatele aplikace zjistí přístupová oprávnění a přizpůsobí tomu jak nabídku, tak vlastní činnost. Uživateli bez příslušných práv je přístup odepřen a je na tuto skutečnost upozorněn informačním oknem. Činnost přihlášeného uživatele je logována jak do aplikačních logů, tak do logů systémových.

5.4.6 Datová struktura plánu vyrozumění

Databáze plánu vyrozumění sestává ze dvou relačních tabulek, které jsou navázány na jak na datovou strukturu organizační struktury, tak na datovou strukturu uživatelů. Jsou to tabulky *vyrozumenilogy* obsahující logy činností jednotlivých uživatelů v rámci aplikace, a *vyrozumeniprava* obsahující nastavení oprávnění jednotlivých správců.



Obrázek 25: ER diagram plánu vyrozumění

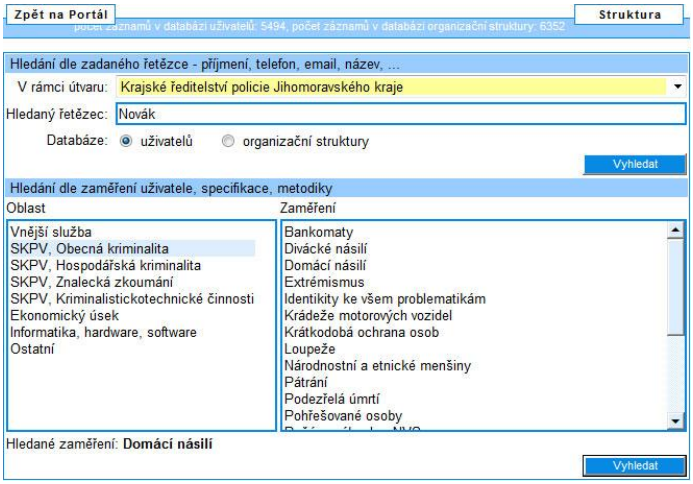
6 NÁVAZNÉ APLIKACE

Informace uložené v organizační struktuře a v databázi uživatelů jsou široce využívány i jinými informačními systémy či aplikacemi v rámci Policie ČR. Praxe ukázala, že soustředění informací do jednoho místa a jejich využívání je efektivní a usnadňuje práci jiným programátorů, kteří je využívají. Přenesením odpovědnosti za aktualizaci dat z administračních pracovišť na jednotlivé uživatele bylo dosaženo mnohem vyšší aktuálnosti uložených informací a snížení chybovosti. Dřívější přístup, kdy se pomocí papírových formulářů obeslalo příslušné administrační pracoviště s požadavkem úpravy údajů, byl nahrazen přímou správou jednotlivých uživatelů. To odbouralo proluky v editaci dat, neboť byl zrušen mezičlánek od uživatele k administrátorovi. Díky organizační struktuře umožňující vypočítat vztahy mezi jednotlivými objekty se mnohem lépe řídí pohyb jakékoliv informace v rezortu Policie ČR, ale navíc je možné informace distribuovat i bez ohledu na jednotlivé uživatele, například stačí uvést útvar a informace se dostane všem uživatelům příslušejícím k danému útvaru. Nahrazení uživatelů funkcemi navíc jednoduchým způsobem umožňuje pracovat i bez znalosti personálního obsazení jednotlivých pracovišť, například pokud je potřeba doručit libovolnou informaci řediteli libovolného útvaru, je tato informace postoupena funkci ředitele a která osoba zastává tuto funkci se stává bezpředmětným. V následujícím textu budou popsány dva informační systémy využívající data z organizační struktury a databáze uživatelů.

6.1 Veřejný výstup kontaktů a organizační struktury

Téměř veškeré údaje uložené v databázích lze získat pomocí veřejných výstupů, kdy je možné potřebné informace velmi rychle zobrazit jednoduchou a uživatelsky komfortní formou. Téměř veškeré proto, že do veřejného výstupu se nedostanou informace osobního charakteru (trvalé bydliště, kontaktní adresa, atd.) a dále jsou z veřejného výstupu vyloučeny skryté (neviditelné) objekty z organizační struktury a skrytí uživatelé. Tedy uživatel má možnost zjistit všechny potřebné služební informace jak ze struktury, tak z databáze osob, které nepodléhají skrytému režimu. Tyto výstupy a hlavně jejich rychlost nalezení je základním požadavkem pro pracovníky krizových pracovišť a operačních odborů při kontaktování kompetentních osob pro řešení nenadálých situacích. Nicméně tyto výstupy využívají všichni pracovníci Policie ČR, neboť je to v tuto chvíli jediný ucelený informační systém v celém rezortu, který tyto informace poskytuje.

6.1.1 Veřejný výstup – specifikace hledání



Obrázek 26: Vyhledávací formulář

Základním vstupem pro získání informací je vyhledávací formulář, kde uživatel specifikuje svoje požadavky a aplikace vyhledá dle vložených parametrů požadované údaje. Uživateli je umožněno specifikovat následující údaje pro hledání:

- **v rámci útvaru** – může být vybrán útvar, který bude ve výstupu předřazen ostatním výsledkům, jinak bude předřazen útvar dle zařazení přihlášeného uživatele. Tímto způsobem je uživateli umožněno diferencovat svůj požadavek na konkrétní organizační článek typu útvar, což v případě mnohonásobného výsledku urychlí nalezení požadované informace. Například při vyhledání informací o uživateli s příjmení „*Novák*“ je v rámci Policie ČR vráceno zhruba 350 osob s tímto příjmením a výsledný výstup je velmi rozsáhlý. Tím, že jsou výsledky rozčleněny do útvarů a předvybraný útvar je ve výstupu koncipován na první místo, je umožněna mnohem rychlejší orientace ve výstupu výsledků.

Další specifikace se týkají řetězce pro hledání osob, kam uživatel vloží libovolný řetězec o délce alespoň tří znaků:

- **dle příjmení** – uživatel vloží alfanumerický text malými písmeny a hledání se omezí pouze na příjmení začínající vloženým řetězcem. Příklad: „*nová*“ nalezne „*Nová, Novák, Nováková, Nováček, ...*“,
- **dle jména a příjmení** – uživatel vloží dva alfanumerické řetězce oddělené mezerou a ve výsledku se zobrazí všechny osoby, jejich jméno a příjmení začíná

jednotlivými řetězci bez ohledu na pořadí. Příklad: „*jan petr*“ nalezne „*Jan Petr, Jan Petráček, Jana Petrová, ...*“ ale i „*Petr Janík, Petra Jandová, ...*“,

- **dle telefonního čísla** – uživatel vloží číselný výraz a ve výstupu se zobrazí všechny osoby, jejich služební telefon začíná vloženým řetězcem,
- **dle kódu zpracovatele** – uživatel zadá alfanumerický text velkými písmeny a ve výsledku budou všichni uživatelé, jejichž kód zpracovatele odpovídá vloženému řetězci,
- **dle emailové adresy** – uživatel zadá alfanumerický řetězec obsahující znak „@“ a ve výsledku budou všichni uživatelé mající ve své služební emailové adrese odpovídající řetězec, přičemž před vlastním hledáním se znak „@“ z vloženého textu vyloučí. Příklad: „*@novak*“ nalezne „*novak@policie.cz, novakova@policie.cz, ...*“,
- **dle pracovní náplně** – uživatel vloží alfanumerický řetězec začínající znakem „+“ (plus) a ve výsledku obdrží všechny osoby, mající v pracovní náplni obsažen vložený řetězec na jakékoliv pozici.

Mnohdy je uživatel při specifikaci vstupního řetězce na pochybách, jak se dané příjmení píše, například foneticky psané příjmení „*Bém*“ se může v psané podobě jevit mnoha způsoby (*Böhm*, atd). Pokud tedy uživatel nezná přesnou podobu hledaného výrazu včetně diakritiky, vloží hledaný řetězec bez diakritických znamének a osoba by přesto měla být nalezena. Například osoba „*Ořůšëłűž*“ bude nalezena, pokud se do pole pro hledání vloží „*oruseluz*“ (tedy pokud se v databázi osob nalézá).

Dalším způsobem hledání je prohledání databáze organizační struktury, kdy uživatel nezná konkrétní osobu, ale zná pracovní pozici, či organizační článek. Hledání je obdobné jako v případě databáze osob, jen je nutné specifikovat oblast, která se má pro hledání použít. Opět je požadován řetězec o délce alespoň tří znaků:

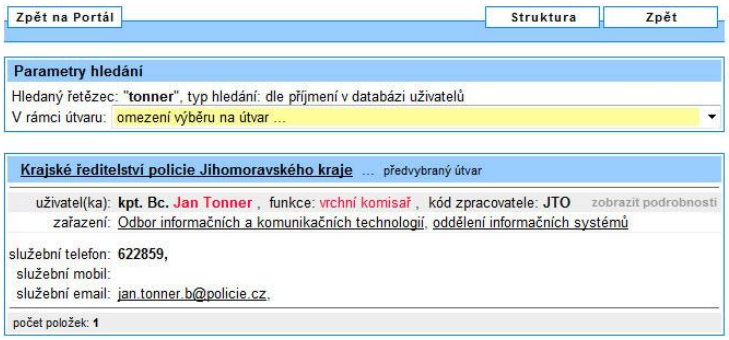
- **dle názvu objektu** – uživatel vloží alfanumerický řetězec malými písmeny a ve výstupu budou všechny objekty obsahující vložený řetězec na libovolném místě. Příklad: „*ředitel*“ nalezne „*ředitel, asistentka ředitele, ...*“,
- **dle telefonního čísla** – uživatel vloží číselný řetězec a zobrazí se ty objekty, jejich služební telefon začíná vloženým řetězcem,
- **dle emailové adresy** – uživatel zadá alfanumerický řetězec obsahující znak „@“ a ve výsledku budou všechny objekty mající ve své emailové adrese odpovídající

řetězec na kterékoliv pozici, přičemž znak „@“ je před vlastním hledáním z řetězce vyloučen. Příklad: „*@ředitel*“ nalezne „*reditel@policie.cz, asistentka.reditele@policie.cz, ...*“.

Posledním způsobem je hledání uživatele dle zaměření, specializace a metodiky, kdy budou nalezeny ty osoby, mající specifikované tyto uvedené informace. Mnoho uživatelů má v rámci svých pracovních povinností definováno zaměření, specializaci nebo gesci za metodickou podporu pro ostatní zaměstnance Policie ČR. Tyto osoby jsou speciálně vyškolené pro úzké specifické požadavky a poskytují pomoc ostatním složkám rezortu, byť do nich služebně nespadají. Tyto osoby lze v rámci veřejného výstupu jednoduše dohledat výběrem ze seznamu specializací či zaměření.

6.1.2 Veřejný výstup – výsledek hledání a detailní informace

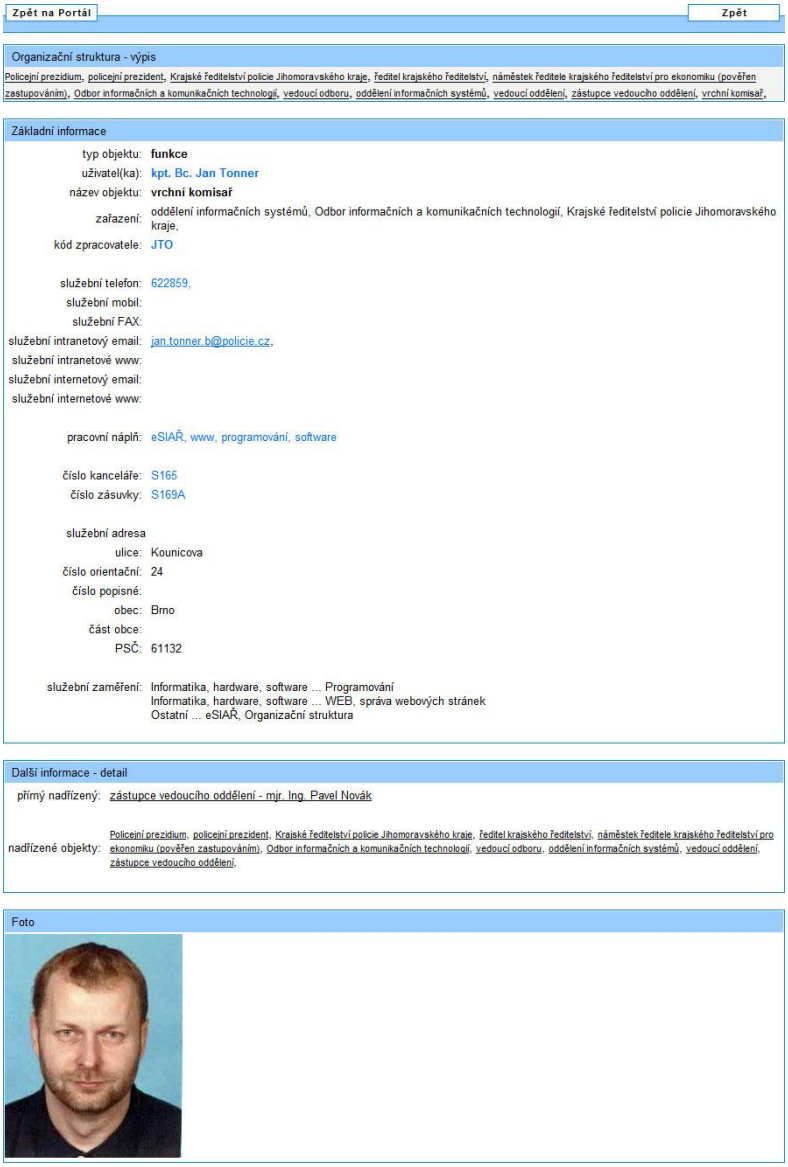
Po specifikaci parametrů hledání je uživateli nabídnut výsledek hledání. Ten obsahuje všechny nalezené položky soustředěné dle jednotlivých útvarů a seřazené podle příjmení či podle názvu objektu na organizační struktuře dle abecedy vzestupně. Základní výstup obsahuje jen ty nejnutnější informace a to parametry hledání, útvar zařazení, identifikační údaje nalezených osob (hodnost, tituly, jméno a příjmení), zařazení osoby v rámci útvaru, služební telefon, služební mobil a služební emailovou adresu. Ve valné většině případů tyto základní informace o osobě postačují uživateli ke zjištění požadovaných informací.



Obrázek 27: Seznam výsledků hledání

Pokud uživateli základní sada informací neposkytne hledaný údaj, je možné kliknutím na „*zobrazit podrobnosti*“ získat kompletní sadu údajů o osobě či objektu na organizační struktuře. V tomto výpise již uživatel nalezne veškeré informace veřejného charakteru s možností jednoduchého pohybu i v rámci organizační struktury, která je nalezené osobě

nadřízená. Velmi snadný způsobem je umožněno zjistit nadřízeného dané osoby, organizační článek, kam nalezená osoba v rámci celého rezortu spadá či si zobrazit jiné osoby spadající do stejného zařazení, tedy přímé spolupracovníky hledané osoby.



Obrázek 28: Detail výsledku

6.1.3 Veřejný výstup – organizační struktura

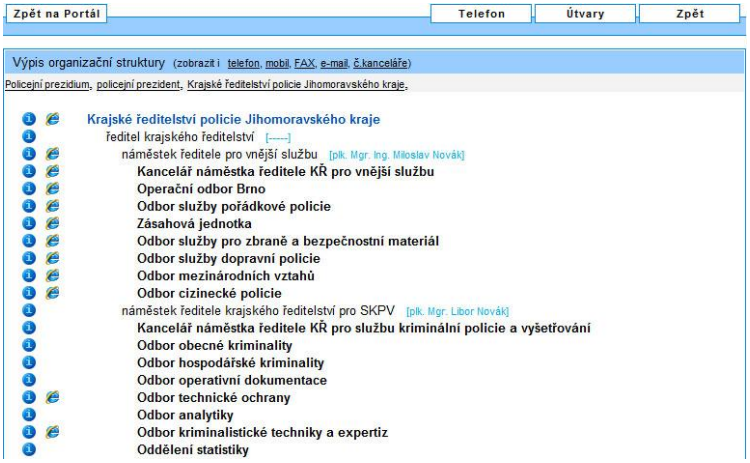
Veřejný výstup neposkytuje pouze informace o jednotlivých osobách či objektech na organizační struktuře, ale umožňuje vypsat i kompletně celou hierarchickou organizační strukturu. Tento celkový pohled na organizaci se využívá k zobrazení celých oddělení, kdy uživatel potřebuje informace, ale neví přesně, kde je má hledat, kdy uživatel ani nezná

rozdělení kompetencí v rámci daného útvaru či odboru, nebo když si uživatel jen potřebuje zobrazit vnitřní strukturu nějakého organizačního článku.

Základním výstupem organizační struktury je seznam všech veřejných útvarů řazený dle abecedy vzestupně.

Obrázek 29: Seznam útvarů

Uživatel kliknutím v seznamu vybere požadovaný útvar, čímž dojde k zobrazení vnitřní struktury vybraného útvaru po jednotlivé odbory.



Obrázek 30: Základní struktura útvaru

Klikáním na jednotlivé objekty v hierarchii se uživatel propracovává postupně hlouběji do organizační struktury vybraného útvaru a je mu umožněno získávat tak přehled o rozdělení útvaru a kompetencích na struktuře přiřazených osob. Každá podřízená vrstva je viditelně odsunuta doprava od nadřízeného objektu, čímž je zřetelně a jednoduše zobrazeno, kdo komu velí či kdo je komu podřízen, přičemž jednotlivé typy objektů jsou pro snadnější identifikaci barevně rozlišeny. Tímto způsobem je možné zobrazit organizační strukturu až na jednotlivé skupiny včetně detailních informací o jednotlivých objektech či osobách na struktuře, kdy výpis detailní informace je totožný s detailním výpisem z procesu hledání.

Navíc je zde umožněn jednoduchý výpis doplňkových informací pro celou zobrazenou skupinu.

Obrázek 31: Struktura oddělení

Veřejný výstup informací o osobách a organizační struktuře je dnes nejvíce využívaným informačním systémem u Policie ČR. Díky jednoduchosti, uživatelskému komfortu a šíři informací byl po svém nasazení doporučen policejním prezidiem k celorezortnímu používání a byly jím nahrazeny všechny obdobné aplikace pracující v rámci jednotlivých krajských ředitelství. Protože byly kompetence na správu osobních informací přeneseny z centrálních administrátorských pracovišť na jednotlivé uživatele, jsou uložené informace mnohem flexibilněji spravovány a snížila se i chybovost uložených dat. Odstranilo se tak vyplňování papírových formulářů a jejich distribuce ke správcům jednotlivých informačních systémů s požadavkem ke změně. Další nezanedbatelnou výhodou je uložení všech informací na jednom místě a využívání těchto dat dalšími aplikacemi. To má výhodu v tom, že při změně jakéhokoliv údaje, je tato změna okamžitě akceptována všemi návaznými informačními systémy a nemusí se tedy změna aplikovat na několika místech v několika aplikacích. Posledním zmíněným kladem je, že nově vznikající informační systémy dle potřeb rezortu již s těmito informace dopředu počítají a tyto údaje jsou včleňovány dle potřeb do nových aplikací.

6.1.4 Zabezpečení veřejných výpisů

Jako u ostatních informačních systémů je i pro přístup k veřejným výpisům potřeba se doménově přihlásit. Po ověření přihlašovacích informací aplikace ztotožní daného uživatele a přizpůsobí mu nabídku předvýběrem útvaru, do jehož gesce přihlášený uživatel spadá. V případě nepřiřazeného uživatele je poskytnuto defaultní nastavení. Činnost přihlášeného uživatele je logována pouze do systémových logů serveru, aplikační logy

informačního systému veřejných výpisů nejsou podporovány, neboť informace zde uložené nepodléhají utajení.

6.2 Aplikace správy a přidělování dokumentů (eSIAŘ – elektronická sbírka interních aktů řízení)

Každá firma či společnost pracuje s dokumenty, ať se již jedná faktury, vnitřní předpisy, právní normy, různá sdělení, apod. Některé dokumenty vyžaduje stát a jeho složky, některé jsou nezbytné pro vlastní činnost společnosti, některé se vztahují k výrobkům (například jakosti), apod., dokumentů je mnoho a mnoho druhů a společnosti je musí zpracovávat a uchovávat. Tato skutečnost pro policii ČR platí dvojnásob, vše je zaznamenané a uložené pro případné pozdější využití. Pro činnost Policie ČR jsou jednotlivými složkami rezortu vydávány dokumenty, které specifikují rozličné problematiky či činnosti.

V minulosti byly jednotlivé dokumenty v rámci Policie ČR vydávány nejednotnou formou především v papírové podobě. Tento způsob prezentace dokumentů znemožňoval jednoduchý přístup libovolnému oprávněnému uživateli, uživatel si musel zjistit, kde je dokument fyzicky uložen a poté o něj na daném pracovišti požádat. Potřeba dokumenty prohlížet ale i vyhledávat nebyla umožněna. Byly sice provedeny pokusy o elektronizaci, ale jednotlivá řešení nebyla vzájemně kompatibilní, neboť jednotlivé útvary si dokumenty ukládaly různými způsoby. Distribuce dokumentů probíhala buď prostým naskenováním a následným odesláním služební poštou, nebo za využití služební emailové pošty. Nevýhodou bylo, že při rozesílání dokumentu o velikosti v řádu desítek až stovek kilobytů (výjimečně megabytů) na desítky až stovky služebních emailových adres vedlo k zahlcení emailových serverů. Seznamování s jednotlivými dokumenty se provádělo formou podpisové doložky, což byl další dokument tentokrát papírový, obsahující seznam pověřených pracovníků, který dotyční pracovníci fyzicky parafovali.

Informační systém eSIAŘ, vytvořený v rámci rezortu, tyto problémy odstraňuje. Všechny dokumenty vytvořené u Policie ČR jsou soustředěny do jediné aplikace, jsou umístěny na jednom serveru a přístup k nim je řízen centrálně. Informace o vzniku nového dokumentu je sice nadále rozesílána služební emailovou poštou, ale již se nerozesílá vlastní dokument, ale pouze http adresa, na které je dokument zpřístupněn. Díky tomu, že informaci lze diferencovat, tak emailovou zprávu obdrží pouze zainteresovaní uživatelé a nedochází k zahlcení poštovních schránek všech uživatelů.

6.2.1 eSIAŘ – obecný úvod

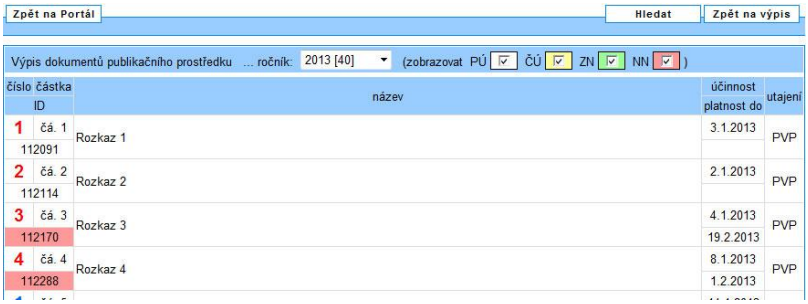
Informační systém eSIAŘ poskytuje vedoucím pracovníkům různého stupně řízení možnost publikovat svoje dokumenty v elektronické podobě formou publikačního prostředku a tyto následně spravovat (novelizovat, rušit, zveřejňovat platná znění, apod.). Každý vedoucí pracovník může vlastnit více publikačních prostředků, každý z nich může lépe charakterizovat uložené dokumenty. Všechny dokumenty jsou uloženy na jednom místě a prostřednictvím vnitřní intranetové sítě jsou k dispozici všem zaměstnancům Policie ČR. Dokumenty lze mezi sebou vzájemně provazovat čímž se usnadňuje uživatelům pohyb po závislých dokumentech. Každý dokument je v systému uložen vždy jen v jednom publikačním prostředku a vlastník dokumentu je zároveň gestorem odpovídajícím za správnost a aktuálnost daného dokumentu. Toto řešení zamezuje duplicitě uložených dokumentů. Publikační prostředek může být veřejný, nebo neveřejný, výběr je ponechán vlastníku, pouze u neveřejného publikačního prostředku je nutné vydefinovat seznam uživatelů majících přístupové oprávnění. Distribuce dokumentu se provádí rozeslání informace s uvedením místa (aktivního odkazu), kde se dokument nachází a tato informace je rozeslána pouze vybraným adresátům uvedeným v organizační struktuře. Publikovaný dokument je uložen tak, jak byl vytvořen, pozdější zásahy do jeho podoby nejsou umožněny. Díky tomu je uživateli zaručeno, že jeho podpis je umístěn pod tím zněním, se kterým se seznámil. Aplikace dále umožňuje vedoucím pracovníkům publikované dokumenty selektivně přidělovat svým podřízeným pracovníkům k prokazatelnému seznámení a kontrolovat jejich průběh. Součástí aplikace je plné fulltextové vyhledávání, což velmi urychluje nalezení požadovaného dokumentu.

6.2.2 eSIAŘ – řadový uživatel

Po přihlášení je uživateli zobrazena úvodní obrazovka rozdělená do dvou částí. Vlevo se nachází osobní seznam publikačních prostředků přihlášeného uživatele, vpravo pak seznam všech publikačních prostředků, které jsou z důvodu přehlednosti soustředěny dle společného útvaru nebo působnosti do složek (podsložek). Osobní seznam má každý z uživatelů vlastní a je mu zobrazen na jakémkoliv počítači v rámci rezortu. Neveřejné publikační prostředky, do kterých nemá uživatel definován přístup, jsou ze seznamu vyloučeny, tedy uživatel se ani nedozví, že takový publikační prostředek existuje. Neveřejné publikační prostředky s právem přístupu jsou označeny červeným vykřičníkem [!].

Obrázek 32: Seznam publikačních prostředků

Po výběru publikačního prostředku se uživatel dostane k obsahu vybraného publikačního prostředku obsahující seznam dokumentů vydaných v aktuálním roce. Výběrem v roletce „*ročník*“ je možné zobrazit seznamy jednotlivých ročníků, klinutím v hlavičce tabulky dojde k jinému seřazení zobrazených dokumentů dle požadovaných parametrů, vývěrem „*zobrazovat*“ dojde k zobrazení či skrytí části seznamu. Například odstraněním výběru NN (neplatné dokumenty) dojde ke skrytí všech červených neplatných dokumentů a ve výpise budou zobrazeny pouze platné dokumenty.

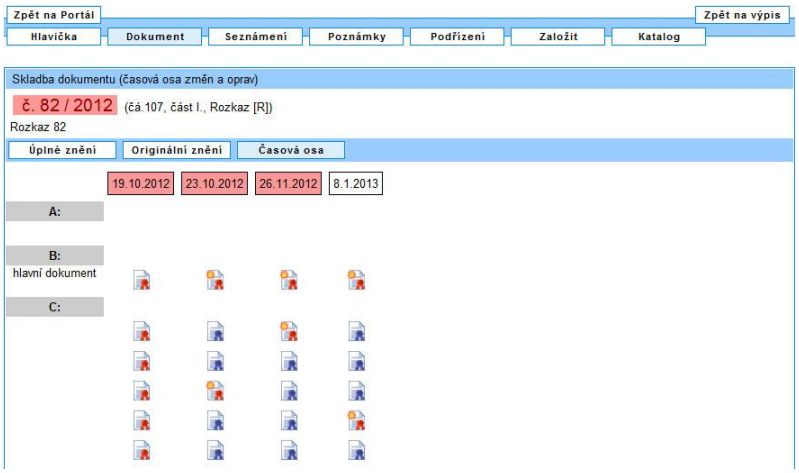


Obrázek 33: Obsah publikačního prostředku

Seznam zobrazuje pouze základní informace o dokumentech vedených v daném publikačním prostředku a to číslo, název, datum účinnosti a stupeň utajení. Výběrem dokumentu si uživatel může zobrazit jeho obsah. Ten již zobrazí kompletní informace o daném dokumentu včetně jeho vlastního obsahu. Detailní informace o dokumentu jsou koncipovány do jednotlivých bloků:

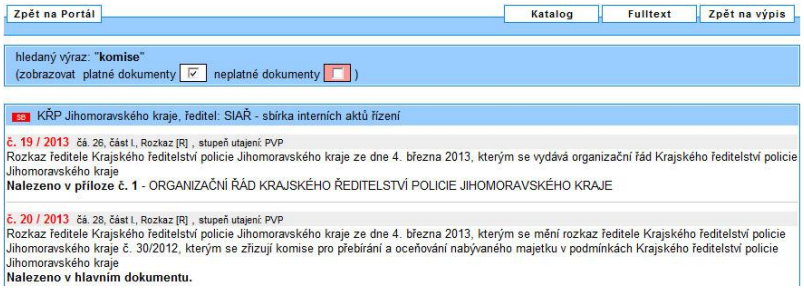
- **hlavička** – obsahuje základní informace o dokumentu, je zde uveden název, platnost a účinnost, novelizace, opravy a rušení a provázanost na jiné dokumenty,
- **obsah** – zde je k dispozici originální znění dokumentu a jeho příloh včetně úplných znění, pokud byl dokument novelizován, také je zde uveden http odkaz na dokument,

- **informace o prokazatelném seznámení** – obsahuje informace o seznámení uživatele s dokumentem, je-li seznámení vyžadováno, kým byl tento požadavek vytvořen a kdy k seznámení došlo,
- **poznámky** – zde je uživateli umožněno editovat vlastní poznámky k dokumentu nebo číst všeobecné poznámky vložené vkladatelem (vlastníkem) či jeho nadřízených,
- **podřízení** – v tomto boku je uživateli umožněno stanovit povinnost seznámení svým podřízeným pracovníkům (pokud je vedoucím funkcionářem), tato povinnost se nestanovuje uživatelům ale podřízeným funkcím,
- **uložení dokumentu mezi oblíbené** – umožňuje uživateli vložit si aktuální dokument mezi oblíbené dokumenty do své příruční knihovny,
- **katalogizace dokumentu** – obsahuje číselníkové informace problematik a zaměření, se kterými je dokument provázán.



Obrázek 34: Detail dokumentu

Systém eSIAŘ uložené dokumenty umožňuje plně fulltextově prohledávat. Uživateli tak v případě potřeby poskytuje nástroj na rychlé vyhledání dokumentu bez toho, aniž by věděl, který dokument potřebuje, případně ve kterém publikačním prostředku je dokument uložen. Hledání může probíhat globálně v celém systému přes všechny publikační prostředky, nebo jen v rámci jednoho publikačního prostředku. Uživatel ve vkládacím poli zapíše hledaný řetězec a ve výsledku obdrží všechny dokumenty včetně jejich příloh obsahující zadaný výraz s informací, zda byl hledaný výraz nalezen v hlavním dokumentu nebo v příloze a jaké.



Obrázek 35: Výsledek fulltextového hledání

Poslední a nejdůležitější informací pro uživatele je uvedena v záložce „*Seznamka*“. Zde se nachází seznam všech dokumentů, u kterých bylo stanoveno některým z nadřízených funkcionářů, že jejich znalost je nezbytná pro výkon funkce, na které je uživatel přiřazen. Tuto povinnost seznámení se s dokumentem může uživateli přidělit kterýkoliv jeho nadřízený dle organizační struktury. Uživatel všechny tyto dokumenty najde na jednom místě i s popisem, které dokumenty a kdy mu byly kterým vedoucím pracovníkem dány k seznámení. Dále zde uživatel nalezne všechny dokumenty, se kterými se seznámil bez ohledu na to, zda mu byly k seznámení přiděleny či nikoliv.

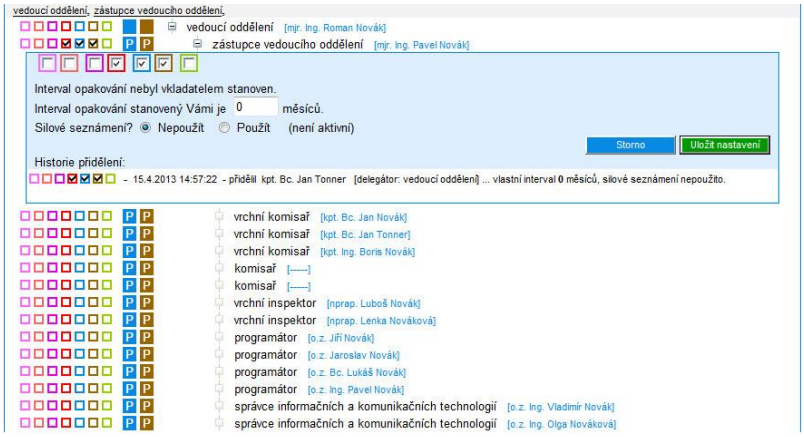
6.2.3 eSIAŘ – vedoucí pracovník

Všechny možnosti práce se systéme eSIAŘ jako má řadový pracovník jsou vedoucímu funkcionáři přístupny také. Navíc mu přibyla možnost či spíše povinnost přidělovat dokumenty k prokazatelnému seznámení svým podřízeným a kontrolovat jejich činnosti. Vedoucí pracovník může u libovolného dokumentu stanovit, že daný dokument je důležitý pro jeho podřízené. Toto rozhodnutí je určeno buď rozdělovníkem daného dokumentu, nebo jen požadavkem vedoucího pracovníka.

Aplikace nabízí několik způsobů jak dokument přidělit a vlastní přidělení je barevně signalizováno, aby vedoucí pracovník měl vizuální kontrolu stavu přidělení.

Zjednodušené základní přidělení – používá se v případě, kdy chce vedoucí pracovník přidělit dokument jedné ucelené skupině svých podřízených. Je vydefinováno 12 základních skupin a vedoucí pracovník zvolí jednu z nich, která nejlépe odpovídá jeho požadavku, a systém již vše nastaví sám. Vydefinované skupiny jsou například: všechny podřízené policejní funkce, všechny podřízené civilní funkce vedoucích pracovníků, všechny přímo podřízené funkce, apod.

Manuální přidělování dokumentů – pokud nestačí zjednodušené základní přidělení, může vedoucí pracovník použít manuální přidělení sestavením vlastní kombinace přidělení. Je zobrazena podřízená struktura s odpovídajícími sedmi manipulačními políčky, jejich vzájemnou kombinací se docílí přesnějšího zacílení přidělení dokumentu na podřízenou strukturu.



Obrázek 36: Přidělení dokumentu

Dále je vedoucímu pracovníku umožněno stanovit interval opakování seznámení, kdy má podřízený pracovní za povinnost se s daným dokumentem seznamovat opakovaně. Například s dokumentem o bezpečnosti práce je potřeba se seznamovat jeden krát ročně. Takový dokument se objeví uživateli v seznamce vždy 14 dní před vypršením stanovené doby opakování s požadavkem opětovného seznámení. Poslední volbou je silové seznámení. To umožní vložit dokument podřízeným uživatelům do seznamky a požadovat opětovné seznámení bez ohledu na to, jestli se s daným dokumentem již seznámili či nikoliv.

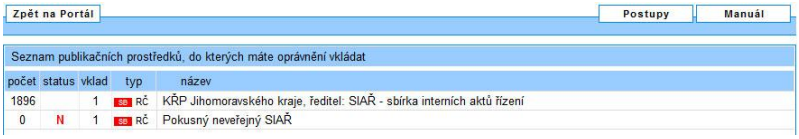
Pro kontrolu seznamování se s dokumentem je vedoucímu pracovníkovi umožněno zobrazit si podřízenou organizační strukturu s jednotlivými pracovníky, kde je zobrazen datum a čas prvního a posledního doménového podpisu příslušejícího danému dokumentu. První podpis značí okamžik, kdy daný pracovník přidělený dokument vzal poprvé na vědomí a seznámil se s jeho obsahem. Druhý podpis je generován v případě dokumentu s periodickou povinností seznamování. Pokud tedy podřízený pracovník daný dokument doménově podepsal poprvé, jsou oba údaje totožné.

Obrázek 37: Kontrola seznamování

6.2.4 eSIAŘ – vkladatel

Tak jako každý významný služební funkcionář má svůj publikační prostředek, tak má každý publikační prostředek své vkladatele. Vkládání dokumentů do publikačních prostředků provádějí proškolení uživatelé s příslušným oprávnění. Standardně se vkladatel může pohybovat v rámci jednoho publikačního prostředku, nicméně jsou vkladatelé obsluhující i více publikačních prostředků. Úkolem vkladatele je umístit do systému schválený dokument, definovat vztahy mezi tímto dokumentem a dokumenty v systému již uloženými a rozeslat informaci zainteresovaným složkám o existenci a umístění nového dokumentu. K tomu využívá vkladatelskou část aplikace eSIAŘ, do které uživatel bez příslušného oprávnění nemá přístup.

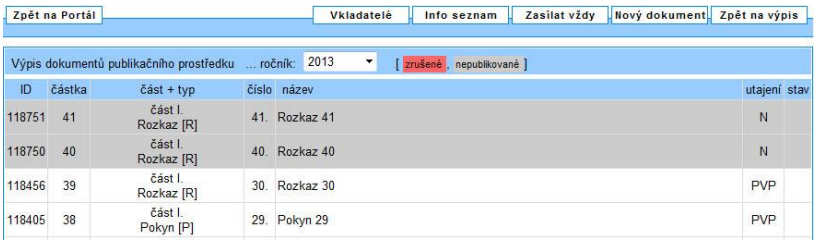
Po doménovém přihlášení je vkladateli nabídnut seznam publikačních prostředků, do kterých mu byl administrátorem systému vytvořen přístup. Tento diferencovaný přístup zabraňuje jiným vkladatelů spravovat cizí dokumenty a umožňuje přenést odpovědnost za spravované dokumenty na úzkou skupinu uživatelů v rámci jednoho publikačního prostředku.



Obrázek 38: Seznam publikačních prostředků vkladatele

Výběrem požadovaného publikačního prostředku je vkladateli zobrazen seznam vložených dokumentů a to jak již publikovaných, tak rozpracovaných, pro rychlejší orientaci vzájemně barevně odlišených. Dokumenty jsou zobrazeny dle ročníků, kdy primárně je vybrán aktuální rok, který je možné změnit v roletce „*ročník*“. Řazení dokumentů je dle požadavků vkladatelů upraveno tak, že nejmladší a rozpracované dokumenty jsou

zobrazeny jako první, protože je zde předpoklad nejčastější práce právě s nimi. Toto řazení lze měnit kliknutím v hlavičce tabulky na příslušný název.



Obrázek 39: Seznam dokumentů

Další administrační práce v rámci aktuálního publikačního prostředku lze provést prostřednictvím nabídky. Vkladateli je umožněno definovat si další uživatele do role vkladatelů bez nutnosti kontaktovat administrátora celého systému. Stačí si vyškolit spolupracovníka pro vkládání dokumentů do aplikace a pak mu přidělit práva přístupu do aktuálního publikačního prostředku. Veškerou odpovědnost tak přebírá stávající vkladatel.

Další možností je vydefinovat emailové adresy pro aktuální publikační prostředek, tedy adresy, na které bude vždy odeslána informace o zveřejnění nového dokumentu, bez ohledu na specifické nastavení příjemců v rámci zveřejňovaného dokumentu, které může být odlišné.

Poslední položkou v nabídce je vytvoření nového dokumentu, kdy se specifikuje pouze číslo a typ dokumentu a tento se jako rozpracovaný objeví v seznamu dokumentů na prvním místě. Při vytvoření nového dokumentu je systémem vygenerované jednoznačné, nadále needitovatelné vnitřní identifikační číslo.

Výběrem dokumentu z nabídky si vkladatel zobrazí detail dokumentu v editačním režimu a je mu umožněno s daným dokumentem pracovat. Je možné editovat veškerá nastavení, názvy, data účinností a platností, vztahů mezi závislými dokumenty, a spoustu jiných nastavení, pouze u vlastního obsahu dokumentu záleží, je-li daný dokument již publikován nebo ne. U nepublikovaného tedy nezveřejněného dokumentu je možné vlastní obsah měnit, u publikovaného již ne. Toto omezení je důsledkem elektronického seznamování se zveřejněným dokumentem, aby bylo zajištěno, že obsah dokumentu se nebude měnit poté, co byl podepsán uživateli. Například bude-li uvedeno v dokumentu, že se mají policisté dostavit v rámci nějakého předem plánovaného zákroku na místo A a poté by byl obsah dokumentu změněn a místo A by bylo nahrazeno místem B, došlo by k tomu, že policisté,

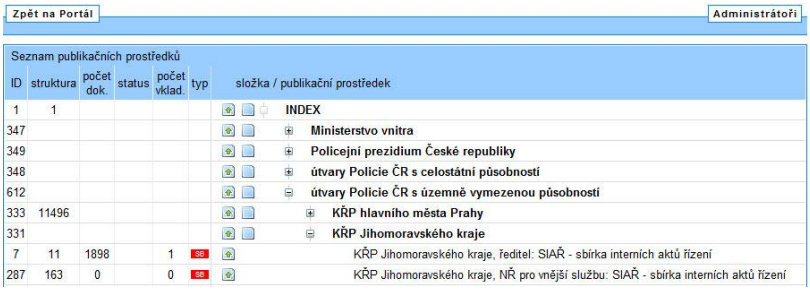
kteří se s dokumentem seznámili před editací, by se dostavili na místo A a policisté, kteří by se s dokumentem seznámili po editaci, by se sešli na místě B. Tomuto problému je zabráněno nemožností editovat vlastní obsah dokumentu po jeho publikování.

Jednou vložený a publikovaný dokument je v systému již navždy uložen. Pokud dokument ztratí platnost, je tato skutečnost uživatelům oznámena grafickým způsobem, ale samotný dokument je v systému nadále přítomen. Díky tomu lze v systému dohledat veškeré dokumenty bez ohledu na jejich stáří a stav. Může nastat situace, že byl do systému vložen a následně publikován dokument, který je chybný. Tato situace není ojedinělá, je zapříčiněna chybou vkladatele nebo změnou originálního (v papírové podobě) dokumentu, kdy změna byla vkladateli oznámena až poté, co původní dokument publikoval. V tomto případě existuje v editačním prostředí možnost změnit stav dokumentu z viditelného na neviditelný. Daný dokument bude nadále zobrazen v editačním rozhraní publikačního prostředku, ale ostatním uživatelů zobrazen nebude, tedy jakoby neexistoval. Tímto způsobem se dá chybný dokument zneviditelnit a namísto něj vydat nový dokument pod stejným číslem, který ale bude mít vnitřní identifikační číslo vygenerované systémem odlišné.

6.2.5 eSIAŘ – administrátor

Administrátor systému eSIAŘ je vyškolený pracovník mající za povinnost vytvářet nové publikační prostředky, spravovat stávající, školit vkladatele do publikačních prostředků a přidělovat jim oprávnění pro vstup, případně řešit vzniklé problémy. Jeho činnost je spíš kontrolní a poradenská. Přestože má administrátor zároveň i práva vkladatelská, publikování dokumentů spadá do pracovních povinností vkladatelů jednotlivých publikačních prostředků.

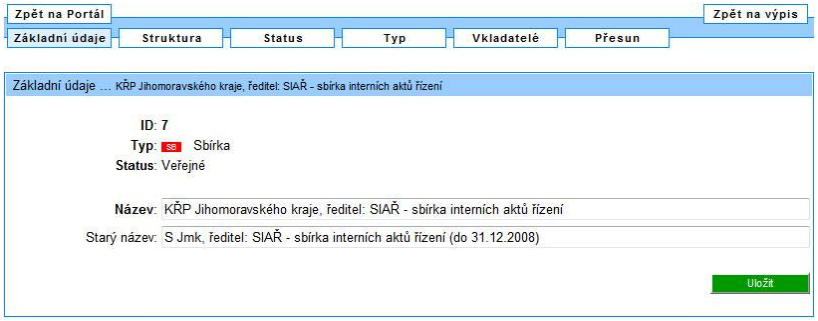
Po doménovém přihlášení je administrátorovi nabídnut seznam všech publikačních prostředků strukturovaně zobrazených. Pohybem po struktuře si administrátor postupně zobrazuje jednotlivé publikační prostředky.



Obrázek 40: Seznam publikačních prostředků – administrátor

V základní nabídce je administrátorovi umožněno vytvořit další administrátory celého systému eSIAŘ. V současnosti je v rámci celého rezortu Policie ČR celkem 5 administrátorů.

Výběrem publikačního prostředku je administrátorovi zobrazen detail daného publikačního prostředku. Zde má administrátor možnost editovat název, přiřazení na organizační strukturu, status veřejného nebo neveřejného publikačního prostředku, typ a definovat vkladatele.



Obrázek 41: Detail publikačního prostředku – administrátor

Systém eSIAŘ umožňuje vytvořit publikační prostředek se statusem veřejný nebo neveřejný. Veřejný publikační prostředek obsahuje dokumenty, k nimž mají přístup všichni uživatelé v rámci celého rezortu Policie ČR. Není na škodu, kdy k dokumentům například z krajského ředitelství ve Zlíně přistupují uživatelé z Brna či naopak. Běžnou praxí je, že dokumenty vydané jedním útvarem jsou převzaty, upraveny a vydány samostatně jiným útvarem. Toto zvyšuje produktivitu práce, kdy nad podobným dokumentem nepracuje souběžně několik týmů zaměstnanců, ale práce je souběžně sdílena a tím pádem i usnadněna a zrychlena.

V případě neveřejného publikačního prostředku je celý jeho obsah zobrazen jen předem striktně definovaných pracovníkům, nebo částem organizační struktury. Uživatel nemající přístup do neveřejného publikačního prostředku ani nezjistí, že takový publikační prostředek vůbec existuje. Status stanoví administrátor a právo přístupu si pak řídí vkladatel daného neveřejného publikačního prostředku. Přístup je definován dvojím způsobem. Prvním je přímé přidělení jednotlivým pracovníkům na základě jejich osobního evidenčního čísla, kdy po přihlášení uživatele do systému je kontrolováno přístupové oprávnění. Druhým způsobem je definování části organizační struktury mající do neveřejného publikačního prostředku přístup. Uživatel přiřazený na organizační struktuře s právem přístupu se do neveřejného publikačního prostředku dostane, ostatní ne. Výhoda druhého způsobu je zřejmá, stačí nastavit práva přístupu na organizační strukturu a dál si již vše řídí systém. Například utajovaný útvar má neveřejný publikační prostředek s nastaveným strukturovým oprávněním. Nový pracovník tohoto útvaru je administrátorem organizační struktury přiřazen na strukturu tohoto útvaru a okamžitě je mu tím zpřístupněn neveřejný publikační prostředek. V případě odchodu tohoto pracovníka z tohoto útvaru a sesazením z organizační struktury, je mu přístup neumožněn.

6.2.6 eSIAŘ – praktické řešení

Vedoucí pracovník mající k dispozici publikační prostředek má potřebu vydat dokument upravující nějakou činnost, například pokyn týkající se plánu vyrozumění. Je kontaktován vkladatel publikačního prostředku, který vytvoří v systému hlavičku nového dokumentu a přidělí jí číslo, které následně sdělí vedoucímu vydávajícímu daný dokument. V systému je vygenerován prostor pro budoucí dokument a je vytvořeno vnitřní identifikační číslo. Daný vedoucí pod číslem sděleným vkladatelem, které je odlišné od vnitřního identifikačního čísla, zpracuje dokument v elektronické podobě (standardně v aplikaci Word), který projde připomínkovým řízení zainteresovaných složek Policie ČR. Poté, co je dokument připomínkován, schválen, vytisknut a podepsán vedoucím pracovníkem případně nadřízeným vedoucím pracovníkem, je elektronická kopie dokumentu předána vkladateli příslušného publikačního prostředku. Ten do místa již systémem předem vygenerovaného prostoru vloží daný dokument, zabezpečí vyplnění všech potřebných a odpovídajících položek a dokument publikuje. V tom okamžiku se dokument objeví všem uživatelům. Poté vkladatel rozešle informaci o publikování všem zainteresovaným útvarům, odborům nebo pracovištím. Jednotliví vedoucí se s dokumentem seznámí a tuto skutečnost potvrdí

svým doménovým podpisem a rozhodnou, je-li zapotřebí, aby daný dokument byl předložen k prokazatelnému seznámení i jejich podřízeným. V nabídce daného dokumentu nastaví, jakým způsobem bude dokument cestovat od jeho funkční pozice na organizační struktuře směrem k jeho podřízeným. Tím příslušným uživatelům tento dokument vloží do „*Seznamky*“, kterou jsou všichni zaměstnanci Policie ČR povinně v průběhu pracovní doby navštívit. Nakonec vedoucí pracovník může provést kontrolu seznamování svých podřízených s daným dokumentem.

6.2.7 eSIAŘ – zabezpečení

Podobě jako u ostatních aplikací je pro přístup do systému eSIAŘ potřeba se doménově přihlásit přihlašovacím jménem a heslem. V případě uživatelského přístupu je nabídka možných operací přizpůsobena přihlášenému a ztotožněnému uživateli, například tím, že jsou mu zobrazeny oprávněné neveřejné publikační prostředky. V případě vkladatelského nebo administračního režimu se kontroluje právo přístupu a uživateli nemajícímu oprávnění je přístup zamítnut formou informačního okna. Ověření přístupových oprávnění se provádí na každé stránce a systém si kontroluje s každým dotazem, je-li uživatel oprávněn obdržet odpověď. Výhodou je minimalizace nebezpečí neoprávněného přístupu či pokusu o něj do zabezpečených částí systému.

6.3 Seznam dalších informačních systémů

Dalšími informačními systémy využívajícími organizační strukturu a databázi uživatelů jakoukoliv formou jsou například:

- **RAUT** – rezervace automobilové techniky – umožňuje rezervovat a následně využívat automobilovou techniku pro služební cesty, kdy uživatel do systému vloží požadavek na dopravní prostředek se specifikací data, času, místa přistavení, místa služební cesty atd. Požadavek je zpracován a v případě schválení nadřízeným orgánem je uživateli dispečerem přidělen příslušný dopravní prostředek dle specifikovaných požadavků,
- **eRecepce** – elektronické vedení návštěv na jednotlivých recepcích v rámci Policie ČR. Informační systém archivující služební návštěvy zaměstnanců rezortu s osobami z civilního sektoru,

- **DPČ** – deník pracovní činnosti – elektronická evidence pracovní činnosti zaměstnanců. Přidělování úkolů metodou shora dolů, od vedoucích pracovníků po jednotlivé podřízené s kontrolou provedeného výkonu,
- **Tachec** – evidence PHM vedené u jednotlivých útvarů. Aplikace umožňuje vedoucím funkcionářům sledovat stav, ceny a odběry jednotlivými podřízenými odbory,
- **služební příprava** – evidence služebních povinností příslušníků Policie ČR. Přihlášením do aplikace si jednotliví příslušníci zjistí termíny školení a výcviků, které jim vyplývají z jejich pracovních povinností,
- a další aplikace využívající organizační strukturu a databázi uživatelů.

7 ANALÝZA RIZIK WEBOVÉHO PROSTŘEDÍ A SQL DATABÁZÍ

Celý provoz informačních systémů formou webových technologií podléhá v čase různým rizikovým faktorů ať už hardwarovým tak softwarovým. Podstatnou součástí rizik jsou pak samotní uživatelé a útoky ze sítě. V rámci vnitřní intranetové sítě Policie ČR, která je striktně oddělena od celosvětové sítě Internet, je zabezpečení proti útokům ze sítě výrazně potlačeno. Opačným extrémem je ztráta údajů uložených v databázích, které jsou nebytně nutné pro činnost policie jako takové, proto je kladen důraz na zabezpečení policejních databází.

Analýza rizik má za úkol odpovědět na otázky jaká aktiva má organizace, jakým hrozbám a rizikům jsou tato aktiva vystavena, jaká je pravděpodobnost zranitelnosti a jaký dopad ztráty aktiv to na organizaci může mít. Pro stanovení se používají následující termíny:

- *aktivum* – vše co má pro organizaci nějakou hodnotu a měly by být chráněno
- *zranitelnost* – slabina aktiva, která může být zneužita hrozbou
- *hrozba* – událost, které může způsobit narušení aktiva
- *riziko* – pravděpodobnost výskytu hrozby
- *opatření* – zabezpečení aktiva před danou hrozbou

7.1 Stanovení aktiv

Z pohledu činnosti informačních systémů je vlastní provoz závislý na:

- *hardware* – jsou na něm uloženy data a vlastní aplikace, a je využíván uživateli formou kancelářských počítačů,
- *software* – což jsou vlastní informační systémy, operační systémy serverů, programy nainstalované na počítačích uživatelů, atd.,
- *datech* – vytvořených aplikacemi a uložených v datovém úložišti,
- *síťových prostředcích* – umožňujících přenos informací ze serveru k uživateli.

Z tohoto pohledu jsou tedy aktivy Policie ČR z pohledu provozování informačních systémů:

- data,
- informační systémy a aplikace instalované na serverech,
- serverový a uživatelský software (operační systém, IIS, Internet Explorer, …),
- serverový a uživatelský hardware (servery, uživatelské počítače, …),
- datová policejní síť.

Z pohledu provozování informačního systému pro podporu krizového řízení je možné z analýzy rizik vypustit datovou policejní síť, jejíž provozování je plně ve správě odborů informační podpory jednotlivých územních celků, které ji udržují v provozuschopném stavu a jsou odpovědné za její fungování. Plánované výpadky datové sítě například z důvodu údržby jsou předem hlášeny a jsou záměrně prováděny v termínech, které jsou z hlediska provozu nevýznamné a mají zanedbatelný vliv na chod Policie ČR jako celku. Tyto zásahy se zpravidla dějí o víkendech nebo v nočních hodinách. Neplánované výpadky například z důvodu poruchy některého aktivního členu sítě jsou řešeny okamžitě analýzou problému a odstraněním závady, například výměnou zařízení. Neplánované výpadky datové policejní sítě jsou zřídka a trvají v řádu několika minut až desítek minut.

Dalším aktivem, které můžeme z pohledu provozování informačních systémů bez úhony vypustit, jsou uživatelské počítače. Opět za jejich správu jsou odpovědné odbory informační podpory jednotlivých územních celků a podobně jako v případě datové policejní sítě, jsou jednotlivé uživatelské počítače pravidelně kontrolovány, případně servisovány nebo nahrazeny novými. Protože informační systémy běží pod HTTP protokolem společně s Active Directory, není v případě nutnosti pro uživatele, který má svůj přidělený kancelářský počítač mimo provoz, problém použít jiný, například počítač kolegy. U Policie ČR neexistuje pracoviště, které by bylo vybaveno pouze jedním počítačem, naopak vybavení Policie ČR výpočetní technikou je na velmi dobré úrovni.

Z důvodů výše popsaných jsou aktiva z hlediska provozování informačních systémů stanovena následovně:

Typ aktiva	Bližší identifikace	Hodnota
Informace	Data v datovém úložišti	1,00
Software	Informační systémy	0,50
	Serverový software	0,25
Hardware	IIS a SQL server	0,50

Tabulka 1: Stanovení aktiv organizace

Z tabulky aktiv je patrné, že nejvyšší hodnotu pro Policii ČR mají samotná data uložená v databázovém prostředí SQL. Nižší hodnotu mají informační systémy a hardware a nejnižší hodnotu má serverový software. Hodnota byla stanovena s ohledem na ztrátu aktiva. Z tohoto pohledu je nejvyšší ztrátou ztráta dat. Data jsou obtížně nahraditelná, při jejich ztrátě včetně záloh by se musela všechna data znovu vytvořit, což by bylo sice možné, ale časově velmi náročné. Všechny údaje uložené v databázích existují i v papírové podobě, tedy ztráta by nebyla pro Policii ČR likvidační, znovuvytvoření by ale stálo velmi mnoho člověkohodin.

Další v pořadí jsou vlastní informační systémy. Ty jsou zálohované ve všech předchozích verzích, tedy případná ztráta by měla za následek pouze novou instalaci a konfiguraci. Pravděpodobnost ztráty jednotlivých aplikací je tedy zanedbatelná, jediným záporem je několika hodinový výpadek provozu informačního systému.

Na stejné úrovni jsou servery jako hardwarové zařízení. Z pohledu provozu by jejich ztráta měla téměř nepodstatný vliv, neboť tato situace by měla za následek pouze přepnutí provozu informačních systémů na existující záložní server, což by z časového hlediska trvalo v řádu několika hodin. Z pohledu ekonomického by tato situace měla mnohem závažnější charakter, neboť by bylo nutné pořídit server nový.

Poslední a nejméně podstatným aktivem je serverový software, což je operační systém Windows Server, případně systém IIS nebo SQL. Všechny tyto programové prostředky jsou uloženy na originálních DVD v několika kopiích a několika pracovištích.

7.2 Identifikace hrozeb a rizik dle aktiv

Hrozbu můžeme definovat jako událost mající negativní vliv na stanovená aktiva. Zranitelnost pak jako pravděpodobnost výskytu hrozby. Z pohledu provozování informačních systémů v návaznosti na definovaná aktiva v předchozí kapitole, můžeme definovat hrozby následovně:

- úmyslné – naplánované a provedené uživatelem,
- neúmyslné – provedené náhodně bez zjevného úmyslu,

dále pak na hrozby vedené proti:

- informacím uloženým v datovém úložišti,
- informačním systémům a instalovanému software,
- serverům a ostatnímu hardware.

Aktivum	Hrozba	Hodnota
Informace (data)	Zneužití dat	1,00
	Úmyslná editace údajů (editace, smazání, vytváření nechtěných dat, …)	0,50
	Neúmyslná editace údajů	0,50
Software	Neoprávněný přístup	0,50
	Pád operačního systému serveru	0,25
	Pád informačního systému	0,25
Hardware	Neoprávněný přístup	0,50
	Porucha IIS nebo SQL serveru	0,25

Tabulka 2: Stanovení míry poškození

Hrozba	Pravděpodobnost
Zneužití dat pomocí IS	0,50
Zneužití dat na SQL serveru	0,50
Hardwarová porucha SQL serveru	0,25
Editace dat pomocí IS	0,12
Editace dat na SQL serveru	0,12
Neoprávněný přístup pomocí IS	0,12
Neoprávněný přístup k serveru	0,12
Pád operačního systému na serveru	0,05
Pád informačního systému	0,05
Hardwarová porucha IIS serveru	0,05

Tabulka 3: Pravděpodobnost vzniku hrozby

Pokud aktiva dáme do vazby s hrozbami, můžeme vydefinovat jednotlivá rizika pro provozování informačních systémů přibližně způsobem, uvedeným v následující tabulce, kde v jednotlivých řádcích jsou uvedena aktiva i s jejich hodnocením a ve sloupcích jsou uvedeny hrozby včetně jejich ohodnocení. Ohodnocení rizika bylo provedeno porovnáním jednotlivých ohodnocení aktiv a hrozeb.

Aktiva	Hrozba	Míra poškození	Pravděpodobnost vzniku
Informace	Zneužití dat	1,00	0,50
	Editace dat	0,50	0,12
	Neoprávněný přístup	0,50	0,12
Software	Pád operačního systému	0,25	0,05
	Pád informačního systému	0,25	0,05
Hardware	Hardwarová porucha serveru	0,25	0,25

Tabulka 4: Analýza rizik

Sumarizace rizik řazených dle míry ohodnocení rizika:

- zneužití dat prostřednictvím informačního systému nebo přímým přístupem k serveru,
- úmyslná nebo neúmyslná editace dat prostřednictvím informačního systému,
- neoprávněný přístup do informačního systému,
- neoprávněný přístup k serveru,
- pád operačního systému serveru nebo software IIS či SQL,
- pád informačního systému na serveru IIS,
- hardwarová porucha serveru.

7.3 Protiopatření k potlačení hrozeb a rizik v závislosti na výši ohrožení

7.3.1 Hrozba zneužití dat

Nejvyšší hrozbou v pohledu provozu informačních systémů je zneužití zpracovávaných informací. Uložená data představují ekonomické hodnoty nejen pro majitele, ale i pro konkurenci. V případě informací uložených v policejních databázích je konkurencí kriminální podsvětí, které má o tyto informace zájem a je ochotno je i náležitě finančně ohodnotit. Toto může mít za následek pokus některých uživatelů informace získat a zhodnotit. Existují dva přístupy k informacím. Prvním je získání informací prostřednictvím informačního systému, druhým je přímý přístup k serverům uloženým na dohledovém pracovišti v Praze.

Protiopatřením v případě první možnosti je nasazení systémového logování na IIS serveru, které ukládá do systémového logu veškeré dotazy provedené prostřednictvím informačních systémů. Tyto logové soubory jsou následně zálohovány a je z nich pravidelně prováděn výstup pro generální inspekci ozbrojených složek. Navíc jsou aplikace pracující s daty soukromého charakteru vybaveny vlastním aplikačním logování, které ukládá datum, čas, uživatele a požadovanou informaci. Tyto aplikační logy jsou pak poskytnuty jednotlivým majitelům informací přímo z prostředí aplikace. Toto opatření sice nezabrání uživatelům s příslušnými právy k přístupu k údajům, ale umožní rychle identifikovat zdroj úniků s následným postihem viníků.

Ve druhém případě přímého přístupu k informacím prostřednictvím serverů je uplatněno pravidlo čtyř očí. Pro přístup k uloženým datům je zapotřebí dvou správců, jeden zná heslo do systému serveru a druhý do databázového systému. Navíc je každý přístup na serverové pracoviště pod dohledem a je veden a archivován přístup pracovníků na takto zabezpečené pracoviště.

7.3.2 Hrozba úmyslné nebo neúmyslné editace dat

Hrozbou s nižším rizikem je záměrná nebo neúmyslná editace uložených dat. Tato hrozba se týká pouze správců jednotlivých informačních systémů, neboť standardní uživatel nemá, kromě vlastních údajů, možnost data editovat. Záměrná chybná editace uložených dat nebyla doposud u Policie ČR řešena, tedy dá se usuzovat, že k této situaci nedochází, nebo

že informace byly jiným správcem navráceny do správné podoby. Neúmyslná editace je jev vyskytující se pravidelně, člověk je tvor omylný. Ať se jedná o editaci, smazání či vytvoření nového chybné údaje, je v možnostech jednotlivých správců uvést data do správného tvaru, tedy v případě smazání jakéhokoliv údaje tento údaj znovu vytvořit, v případě chybné editace provést následně správnou editaci a v případě vytvoření nového údaje tento údaj smazat. U informací, které byly v průběhu provozování informačních systémů vyhodnoceny jako kritické, je mazání neumožněno, tyto informace jsou pouze označeny jako smazané a nadále se ve výstupech neobjevují, přesto nadále v databázích zůstávají. V případě, že správce smaže takovou informaci, je snadné ji opět vrátit do systému jednoduchou změnou položky v databázi. Příkladem je zhasnutí uloženého dokumentu v systému eSIAŘ, kdy uživatelé tento dokument již nenajdou, ale v databázi je tento dokument uložen napořád.

Podobně jako u hrozby zneužití je možné dohledat uživatele, který editaci, smazání či vytvoření libovolného údaje provedl a kdy tato událost nastala. Tyto události jsou ukládány do systémového logu IIS serveru, případně do aplikačních logů jednotlivých informačních systémů. Z aplikačního logu je navíc možné zjistit hodnotu údaje před editování a tedy provést opětovnou editaci na původní správnou hodnotu.

Zabezpečení proti nesprávné editaci není možné i z toho důvodu, že uživatel mající příslušná přístupová práva je díky tomu oprávněn editaci provést a pokud je editovaný údaj v rámci daných mezí a kritérií, neumí aplikace určit, je-li editovaný údaj správný či nikoliv.

7.3.3 Hrozba neoprávněného přístupu do informačního systému

Hrozba neoprávněného přístupu spočívá v používání přístupového oprávnění neoprávněným uživatelem. Jedná se především o zneužití identifikačních údajů při doménovém přihlášení do informačních systémů. Způsoby jsou dva. V prvním případě uživatel dobrovolně sdělí své identifikační přihlašovací údaje jiné osobě, ve druhém případě se uživatel neodhlásí z domény na pracovním počítači, odejde od něj a jiný uživatel tak může využít aktuálního přihlášení. Dalším možným způsobem je uhádnutí hesla, což je ale při současné politice nastavení a omezení pro hesla téměř nemožné.

Přístup do jednotlivých aplikací je řízen dvojím způsobem a to doménově a aplikačně. Každý uživatel má vytvořen v policejní doméně svůj jednoznačný uživatelský účet. Dle

rozkazu policejního prezidenta má každý uživatel povinnost tento doménový účet chránit před zneužitím pravidelnými změnami hesla a ochranou tohoto hesla před jinými osobami. Nedodržení tohoto nařízení je následně řešeno dle závažnosti a dle rozhodnutí nadřízenými složkami. Na doménovém serveru jsou uplatněny restrikce na hesla. První je časová, kdy platnost hesla po určité době vyprší a uživatel je vyzván k jeho změně. Druhá restrikce je na velikost hesla, kdy je vložené heslo kontrolováno na délku. Třetí restrikce je na obsah hesla, kdy uživatel při zadávání nového hesla musí využít malá písmena, velká písmena, čísla případně speciální znaky. Poslední restrikce je na opakování hesel, kdy systém pozná, že uživatel vložil jako heslo nové již jednou heslo použité.

7.3.4 Hrozba neoprávněného přístupu k serveru

Tato hrozba byla popsána v kapitole zneužití dat přímým přístupem k serveru, kdy je přístup na zabezpečené pracoviště pod dohledem a využívá se pravidla čtyř očí. Tímto způsobem je zabezpečena hrozba zneužití dat tak hrozba neoprávněného přístupu k některému ze serverů.

7.3.5 Hrozba pádu operačního systému serveru nebo informačního systému

Další hrozbou při provozu informačních systémů je softwarová chyba buď v operačním systému serveru, nebo chyba v informačním systému. Tato situace může nastat v případě neodborné manipulace správce serveru, ale i procesem mimo činnost správce.

Operační systém je pravidelně aktualizován bezpečnostními soubory vydanými přímo firmou Microsoft. V minulosti již nastal případ, kdy po provedení aktualizace operačního systému došlo k pádu IIS a tedy k zastavení činnosti informačního systému. Tato situace se okamžitě odrazila v činnosti jednotlivých uživatelů a správce IIS serveru provedl deinstalaci bezpečnostní aktualizace a reinstalaci IIS. Celá operace trvala cca 2 hodiny a závažným způsobem neovlivnila chod Policie ČR jako celku. Proti této hrozbě není žádné protiopatření, dokud bude systém Windows takový, jaký je, žádná obrana proti pádu operačního systému neexistuje.

Pád informačního systému je zapříčiněn nedostatečným odladěním nových komponent či funkcionalit. Nastává většinou v okamžiku přechodu mezi novými verzemi jednotlivých aplikací. Jako vše i informační systém prochází vývojem, kdy se přidávají nové funkcionality, přepracovávají se staré, některé se ruší, apod. Každá nová část aplikace se

v první fázi testuje na zkušebním serveru, kdy se provádí kontrola její stability, komunikace s ostatními částmi systému, testují se reakce na vkládaná data, atd. Není v silách programátorů odladit všechny nedostatky, které mohou během provozu nastat, uživatelé vždy přijdou s chybou, která vývojové pracovníky ani nenapadla.

Protiopatřením je důsledná záloha všech předchozích verzí jednotlivých aplikací, aby v případě pádu byl možný rychlý návrat k předchozí bezchybně fungující verzi systému. Pro tento případ hrozby jsou uloženy záložní kopie všech verzí jednotlivých informačních systémů na dvou místech, a to v Praze a Brně.

7.3.6 Hrozba hardwarové poruchy IIS nebo SQL serveru

Poslední analyzovanou hrozbou při provozu informačních systému je hardwarová porucha nebo výpadek jednoho ze serverů, buď aplikačního IIS, nebo databázového SQL serveru. Přestože jsou servery pravidelně kontrolovány a je na nich prováděna údržba, vlivem okolního prostředí může dojít k poruše. Veškerý hardware je náchylný na podmínky provozu, záleží na umístění serverů, na teplotě okolí, na prašnosti prostředí, na relativní vlhkosti, a na mnoha dalších specifických faktorech. Servery určené pro provoz informačních systémů pro podporu krizového řízení mají vytvořeny náležité podmínky, mající příznivý vliv na jejich chod. Oba zmiňované servery jsou umístěny na zabezpečeném pracovišti obsahujícím zařízení na sledování a regulaci okolního prostředí. Jedná se především o udržování teploty a vlhkosti okolí. Prostor umístění dále podléhá dozorovému režimu s omezeným přístupem. Přesto může nastat situace hardwarové poruchy některého ze serverů.

V případě situace hardwarové poruchy serveru je k dispozici náhradní server, sloužící jako záloha, na nějž by byla provedena okamžitá instalace potřebného softwarového vybavení. Časová náročnost operace by byla, jak v případě poruchy IIS serveru, tak v případě poruchy SQL serveru, v řádu několika hodin včetně testování funkčnosti. Tento časový interval není z hlediska provozování informačních systémů nijak fatální, údaje potřebné pro případný zásah u mimořádné události jsou archivovány v papírové podobě na pracovištích operačního střediska nebo krizového oddělení.

Nutností pro potlačení hrozby hardwarové havárie serverů je zálohování datových a aplikačních zdrojů. SQL server má tuto politiku nastavenu na pravidelné zálohování databází 2 krát denně, kdy první záloha je rozdílová a druhá záloha prováděná v nočních

hodinách je kompletní, přičemž rozdílová 12 hodin stará záloha je následně smazána. Zálohy jsou umístěny ve dvou datových centrech a to v Praze a Brně. Zálohy jsou uchovávány několik dní zpětně, pro případ nutného zásahu do starších dat. V případě IIS serveru je zálohování popsáno v předchozí kapitole hrozby pádu informačního systému, kdy jsou zálohovány všechny verze všech informačních systému opět na dvou zálohových pracovištích v Praze a Brně.

Zabezpečené pracoviště, kde jsou servery fyzicky umístěny je pod neustálým 24 hodinovým dohledem pracovníků informační podpory policejního prezídia, majících k dispozici všechny prostředky umožňující jim zvládnout jakoukoliv havárii hardwarového ale i softwarového charakteru.

ZÁVĚR

Cílem této práce bylo popsat činnosti operačního odboru a krizového pracoviště v návaznosti na informační systémy provozovanými u Policie ČR, pro řízení ostatních složek rezortu, které se podílejí na odstraňování následků vzniklých krizí a mimořádných událostí. Jsou zde charakterizovány a popsány složky Policie ČR zapojené do integrovaného záchranného systému a jejich oblasti působnosti. Vzhledem k rozsáhlosti dané problematiky nebylo možné v rámci této práce charakterizovat všechny možné stavy krizí a mimořádných událostí, neboť ovlivňujících faktorů je nezjistitelné množství. Proto je práce spíš všeobecným popisem činností, kterými se operační středisko a krizové pracoviště musí zaobírat, aby zabránilo či minimalizovalo škody na životech, zdraví nebo majetku.

V první části byly charakterizovány jednotlivé složky Policie ČR zapojené do řešení vznikajících krizí či mimořádných událostí. Jsou zde popsány krizové stavy, mimořádné události a postupy, kterými jsou tyto nepříznivé stavy postupně eliminovány formou krizových scénářů. Dále jsou v první části charakterizovány i složky záchranného systému, se kterými Policie ČR spolupracuje a vzájemná koordinace záchranných prací všech těchto zainteresovaných složek. Nakonec jsou v první části teoreticky popsány použité technologie pro rezortní informační systémy.

Ve druhé části byly detailněji charakterizovány jednotlivé informační systémy a jejich používání včetně obrázků jednotlivých obrazovek. Byly rozebrány jednotlivé uložené informace a vztahy mezi nimi. Dále je zde popsán jak uživatelský tak i správcovský přístup k informačním systémům. Jsou zde demonstrovány jednotlivé operace umožňující data ukládat a následně vytěžovat. Jsou popsány různé přístupy dle různých oprávnění, změny nabídek a pracovních postupů dle ztotožněného uživatele. Jsou zde rozebrány vtahy mezi jednotlivými závislými informačními systémy a využívání informací jinými aplikacemi. Nakonec je ve druhé části charakterizováno zabezpečení uložených informací před zneužitím nebo neodbornou manipulací.

Snahou práce bylo demonstrovat a nastínit práci složek Policie ČR zainteresovaných na zvládání krizových nebo mimořádných událostí, tedy situací, které jsou pro obyvatelstvo nepříznivé a nežádoucí. Tyto situace vznikají náhle a jejich dopad je také díky Policii ČR minimalizován a mnohdy i eliminován v samém počátku. Díky stále lepší informovanosti a vzájemnému propojení všech složek integrovaného záchranného systému se postupem času

daří nepříznivé situace nejen likvidovat, ale i předvídat a tak bránit jejich vzniku. Proto je Policie ČR potažmo celý integrovaný záchranný systém potřebnou složkou našeho společenského systému a její rozvoj je v dnešní době sociálních a klimatických změn nutností.

CONCLUSION

The aim of this study was to describe the activities of the operating department and emergency department in relation to the information systems operated by the police to control other components of the resort, which is involved in removing the consequences during arising crises and emergencies. There are characterized and described the components of the police which are involved in the integrated rescue system and their scope. Given the scale of the problems in this work has not been possible to characterize all the possible states of crises and emergencies as the number of influencing factors is undetectable. Therefore, the work is rather general description of activities in which the operations center and emergency department must entertain, to prevent or minimize damage to life, health or property.

In the first part there were described the individual components involved in the police responses to emerging crises or emergencies.There are described states of emergency, emergencies and procedures to these adverse conditions gradually eliminated through crisis scenarios. Furthermore, the first section describes the components of rescue system which cooperate with the police and the coordination of all these stakeholders. Finally, in the first part of the theory there are described the technologies used for departmental information systems.

In the second part there were characterized in detail the various information systems and their use, including pictures of each screen. They were focused on different stored information and the relationships between them. It is described here as a user and an administrator access to the information systems. There is presented here how each operation allows data to be stored and subsequently extract. It describes the different approaches by different permissions, change menus and workflows according to identified user. There are analyzed External Relations between dependent information systems and use of information by other applications. Finally, the second section describes the security of stored information from misuse or improper handling.

The aim of the study was to demonstrate and outline the components of thepolice work involved in the management of crisis or emergency situations, ie situations that are unfavorable and undesirable for population. These situations arise suddenly, and their impact is minimized thanks to the Police and is often eliminated at the very beginning. With an ever better information and interconnection of all components of the integrated

rescue system we over time manage not only to destroy the adverse situation, but also to predict and thus prevent their occurrence. Therefore, the police hence the whole integrated rescue system is the necessary component of our social system and its development is nowadays, in social and climate ganges, necessary.

SEZNAM POUŽITÉ LITERATURY

[1] LUBBERS, Peter, Brian ALBERS a Frank SALIM. HTML5: programujeme moderní webové aplikace. Vyd. 1. Brno: Computer Press, 2011, 304 s. ISBN 978-80-251-3539-6.

[2] SCHURMAN, Eric M a William J PARDI. Dynamické HTML v akci. Vyd. 1. Praha: Computer Press, 2000, xvii, 421 s. ISBN 807226401x.

[3] MIKLE, Pavol. XDHTML: HTML, XHTML, DHTML : úplná přesná referenční příručka. Vyd. 1. Brno: Zoner Press, 2004, 206 s. ISBN 8086815013.

[4] VÁCLAVEK, Petr. JavaScript: hotová řešení. Vyd. 1. Brno: Computer Press, 2003, 255 s. ISBN 8072268546.

[5] FLANAGAN, David. JavaScript: kompletní průvodce. 2. aktualiz. vyd. Praha: Computer Press, 2002, 825 s. ISBN 80-7226-626-8.

[6] HILLIER, Scot a Daniel MEZICK. Programování Active Server Pages: přel. z angl. orig. Praha: Computer Press, 1998, 291 s.+CD ROM. ISBN 8072261185.

[7] VIEIRA, Robert. SQL Server 2000: programujeme profesionálně. Vyd. 1. Praha: Computer Press, 2001, xxxii, 1170 s. ISBN 8072265067.

[8] ŠIMŮNEK, Milan. SQL: kompletní kapesní průvodce. 1. vyd. Praha: Grada, 1999, 247 s. ISBN 8071696927.

[9] Interní akty řízení Policie ČR.

[10] Zákon č. 240/2000 Sb. O krizovém řízení a o změně některých zákonů (krizový zákon) ze dne 28. června 2000 ve znění pozdějších předpisů je mimořádná událost, při níž je vyhlášen stav nebezpečí, nouzový stav, stav ohrožení státu nebo válečný stav.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory – adresářová služba umožňující zabezpečení aplikací a dat
ASP	Active Server Page – dynamické programování na straně serveru
CDO	komponenta operačního systému Windows umožňující rozesílání emailových zpráv
CSS	Cascading Style Sheets – jazyk pro popis zobrazení objektů v HTML stránce
CSV	Comma-Separated Values – jednoduchý souborový formát pro výměnu tabulkových dat
ČR	Česká republika
eSIAŘ	elektronická Sbírka Interních Aktů Řízení – informační systém provozovaný v rámci Policie ČR
Excel	tabulkový procesor od firmy Microsoft, který je součástí kancelářského balíku Microsoft Office
GB	Giga bajty – jednotka kapacity datového úložiště
Gbit	Giga bity – jednotka rychlosti přenosu počítačové sítě
GET	dotazovací metoda HTTP protokolu
HDD	Hard Disk Drive – pevný disk
HTML	Hypertext Markup Language – značkovací jazyk určený pro formátování stránek v prostředí Internetu
HTTP	Hypertext Transfer Protocol – protokol pro přenos dokumentů ve formátu HTML
HTTPS	Hypertext Transfer Protocol Secure – zabezpečený protokol pro přenos dokumentů ve formátu HTML
ID	označení pro automaticky vytvořený identifikační klíč
identity	příkaz SQL pro automatické vytváření identifikačního klíče
IIS	Internet Information Services – softwarový webový server
IZS	Integrovaný záchranný systém

JS	Java Script – multiplatformní programovací jazyk
Policie ČR	Policie České republiky
POST	dotazovací metoda HTTP protokolu
RAID	vícenásobné diskové pole levných nezávislých pevných disků
RAM	Random-Access Memory – paměť s přímým přístupem
SQL	Structured Query Language – standardizovaný dotazovací databázový jazyk
SSL	Secure Sockets Layer – zabezpečení síťové komunikace šifrováním a autentizací
TB	Tera bajty – jednotka kapacity datového úložiště
TCP	Transmission Control Protocol – internetový protokol
TSL	Transport Layer Security – předchůdce SSL – zabezpečení síťové komunikace šifrováním a autentizací
T-SQL	Transact-SQL – rozšíření pro SQL
Word	textový procesor od firmy Microsoft, který je součástí kancelářského balíku Microsoft Office
WWW	World Wide Web – označení pro aplikace internetového protokolu HTTP

SEZNAM OBRÁZKŮ

SEZNAM TABULEK