Systém zabezpečení ochrany osobních údajů občanů v informačním systému veřejné správy

Bc. Veronika Zámečníková

Diplomová práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

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

Jméno a příjmení:	**Bc. Veronika Zámečníková**
Osobní číslo:	**A16314**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Systém zabezpečení ochrany osobních údajů občanů v informačním systému veřejné správy**
Téma anglicky:	**Citizens' Personal Data Protection Systems in Public Administration Information Systems**

Zásady pro vypracování:

1. **Zpracujte rešerši vztahující se k problematice zvoleného tématu včetně legislativních norem.**
2. **Popište strukturu informačního systému úřadu práce.**
3. **Analyzujte současná rizika zabezpečení informačního systému úřadu práce s důrazem na osobní údaje.**
4. **Zhodnoťte současný stav informačního systému a navrhněte vhodný způsobu implementace ochranných mechanismů.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JAŠEK, Roman.Ochrana znalostí a dat v podnikových informačních systémech. Zlín: Univerzita Tomáše Bati, Fakulta managementu a ekonomiky, 2002, 115 s. ISBN 807-31-8095-2.**
2. **JAŠEK, Roman, Miroslava DOLEJŠOVÁ a Pavel ROSMAN. Informační technologie ve veřejné správě. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 183 s. ISBN 978-80-7318-607-4.**
3. **DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.**
4. **POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s. Vysokoškolské učebnice. ISBN 80-86898-38-5.**
5. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.**

Vedoucí diplomové práce: **doc. Ing. Jiří Gajdošík, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. prosince 2017**

Termín odevzdání diplomové práce: **28. května 2018**

Ve Zlíně dne 8. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Jméno, příjmení: Bc. Veronika Zámečníková

Název bakalářské/diplomové práce: Systém zabezpečení ochrany osobních údajů občanů v informačním systému veřejné správy

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 připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- 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/bakalářské 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, dne …….

podpis diplomanta

ABSTRAKT

Diplomová práce se zabývá problematikou ochrany osobních údajů občanů v informačním systému veřejné správy. Teoretická část rešeršní metodou objasňuje základní pojmy spojené s bezpečností informací, informačním systémem veřejné správy a základní legislativou. Dále se zabývá teorií analýzy rizik, zranitelností a následným zabezpečením informačního systému. Praktická část představuje analyzovaný objekt veřejné správy se zaměřením na tamější informační systém, jeho strukturu a způsob zabezpečení spravovaných dat. Dále řeší analýzu rizik základních činností úřadu práce spojených převážně se zpracováním osobních údajů občanů s cílem navrhnout vhodný způsob implementace ochranných mechanismů.

Klíčová slova: bezpečnost, informační systém, veřejná správa, osobní údaje, občan

ABSTRACT

The thesis deals with the protection of citizens' personal data in the public information system. The theoretical part of the search method explains basic concepts related to information security, public information system and the basic legislation. Further deals in theory of risk analysis, vulnerability and security information system. The practical part represents the analysed object of public administration and is aimed at the public administration information system, its structure and security of data. It also solves risk analysis of the basic activities of the employment office related predominantly with the processing of personal data of citizens with a view to proposing appropriate to implement protection mechanisms.

Keywords: security, information system, public administration, personal data, citizen

Tímto bych ráda poděkovala mému vedoucímu diplomové práce, doc. Ing. Jiřímu Gajdošíkovi CSc., za odborné vedení při tvorbě této diplomové práce. Děkuji také Ing. Dušanovi Homzovi, správci informačního systému, za cenné rady, poskytnuté informace a podklady v oblasti informačního systému úřadu práce.

Další poděkování patří mé rodině a blízkým, kteří mne během studia velmi podporovali a povzbuzovali.

OBSAH

ÚVOD

Pro svoji diplomovou práci jsem si zvolila téma Systém zabezpečení ochrany osobních údajů občanů v informačním systému veřejné správy. Uvedená téma mne zaujala z toho důvodu, že sama ve veřejné správě pracuji a s problematikou ochrany osobních údajů občanů se v praxi denně setkávám.

Diplomová práce je rozdělena do dvou navzájem navazujících částí. Úvod teoretické části vysvětluje základní pojmy týkající se bezpečnosti informací a informačního systému zaměřeného na veřejnou správu. Dále je zde uveden nejzákladnější právní rámec týkající se řešené problematiky. Další bod popisuje teorii analýzy rizik informačního systému s identifikací jednotlivých přístupů a samotnou bezpečnostní politiku informačního systému. Závěr teoretické části upozorňuje na možné hrozby informačního systému, které mají za následek oslabení jeho bezpečnosti, a následně definuje efektivní možnosti zabezpečení informačního systému z několika základních hledisek.

V praktické části se diplomová práce zaměřuje na konkrétní objekt veřejné správy, jímž je úřad práce. Zabývá se jeho základním představením z hlediska politiky, náplně činnosti a fyzickým uspořádání konkrétního pracoviště v Kyjově. Okrajově zmiňuje též podstatné aspekty informační a spisové bezpečnosti s následným stručným postupem samotného procesu podání žádosti o zprostředkování zaměstnání a podpory v nezaměstnanosti. Další kapitola je již věnována struktuře informačního systému úřadu práce jako takové. V následujících úsecích je rozebrána oblast antivirové ochrany informačního systému a elektronické pošty, zálohování dat a dále samotný vliv složení zaměstnanců úřadu práce na bezpečnost zpracovaných dat.

Z výčtu nejvýznamnějších činností, spojených zejména se zpracováním osobních údajů občanů, prováděných na úřadu práce, jsem za pomoci jednoduché bodové metody PNH vytvořila a následně vyhodnotila analýzu rizik. V závěru práce jsem zhodnotila analyzovaný informační systém a následně uvedla navržená bezpečnostní opatření vedoucí ke zvýšení ochrany osobních údajů občanů.

I. TEORETICKÁ ČÁST

1 BEZPEČNOST

Pod pojmem bezpečnost si můžeme představit širokou škálu oblastí. V každém případě se ale shodneme v tom, že bezpečnost znamená určitou míru jistoty, která snižuje pocit ohrožení. Důvody a metody zabezpečení byly v průběhu dějin proměnlivé, předmětem bezpečnosti a ochrany byly však vždy následující skupiny:

- zdraví a život,
- majetek,
- informace a znalosti na těchto informacích založené.

Výše uvedené skupiny spolu v řadě případů úzce souvisí a prolínají se. Jako zvláštní skupinu identifikujeme poznatky a znalosti získané na základě informací. Jedná se o takové znalosti a informace, které nejsou běžně dostupné. Nejsou to tedy veškeré informace, ale pouze takové, které mají významnou hodnotu pro jejich uživatele.

Řešení bezpečnostní problematiky vždy vyžaduje posouzení individuálních podmínek konkrétních subjektů a jejich zájmů. Každý subjekt je povinen odpovědět na následující otázky:

- zda a co má být chráněno,
- před čím má být předmět ochrany chráněn,
- jakým způsobem a jakými prostředky bude ochrana zajištěna.

1.1 Informační bezpečnost

Informační bezpečnost je relativně nový pojem. Jeho počátky sahají do první poloviny osmdesátých let, kdy je vyžadován přesun dat všeho druhu do privátních výpočetních systémů.

„Informační bezpečnost chápeme jako zodpovědnost za ochranu informací během jejich vzniku, zpracování, ukládání, přenosu a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot.“

1.2 Cíle informační bezpečnosti

Za základní cíl informační bezpečnosti považujeme ochranu a eliminaci hrozeb včetně jejich dopadů. Mezi možné hrozby řadíme například:

- kompromitace,
- nedovolená modifikace,
- zneužití citlivých údajů,
- užití klamných dat,
- nepřesná interpretace hodnot,
- neoprávněný přístup k hmotným a nehmotným hodnotám,
- únik informací. [1]

Zajištění a řízení bezpečnosti informací patří k nejdůležitějším úkolům organizace. Všechny organizace musí vybudovat systém bezpečnosti a o tento systém se usilovně starat. Při rozhodování ohledně zajištění bezpečnosti informací je nutné zabývat se:

- vzájemným propojováním různých odvětví života pomocí informačních technologií,
- rozvojem informačních technologií,
- způsoby a technikami přenosu dat v sítích a jejich možného ohrožení. [2]

2 INFORMAČNÍ SYSTÉM

V širším pojetí můžeme za informační systém (IS) považovat jakýkoliv systém, jehož funkcí je tvorba, získávání, přenos a užití informací.

Informační systém je definován jako soubor programů (software), technických prostředků (hardware) a metod, lidí (orgware) zabezpečujících sběr, přenos, uchování a zpracování dat, za účelem tvorby a prezentace informací pro potřebu uživatele. Toto komplexní pojetí se v užším významu nazývá systémem zpracování dat a informací, a je užíván za účelem označení systému programů pro práci s daty.

Informační systém se tedy vyznačuje spojením hardwaru, softwaru a orgwaru s cílem zpracovat a uchovat informace ke zvyšování efektivity lidské činnosti. IS považujeme i za systém umožňující využití více disciplín, složitý systém zahrnuje množství různých aspektů a dimenzí.

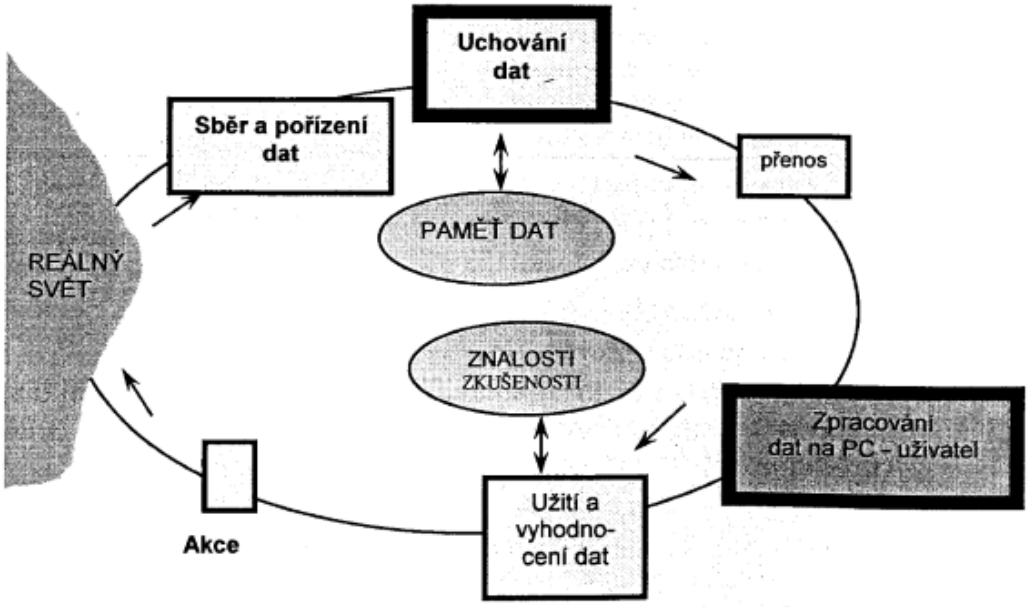
2.1 Pojetí informačního systému

Informační systém můžeme pojmout následujícím způsobem:

- systém zpracování dat,
- systém pravidel a způsobů řízení v určité organizaci,
- jeden ze systémů v každé organizaci,
- systém zahrnující aspekty více disciplín.

2.1.1 Systém zpracování dat

Informační systém zpracovává data popisující objekty a procesy a poukazuje na to, že tyto data musí nějakým způsobem vzniknout. K příjemci informace se dostávají zprostředkovaně, po průběhu několika fázemi. Jelikož všechny tyto fáze neprobíhají v jedné lokalitě, vstupuje mezi ně samostatná fáze přenos dat. [1]



Obr. 1. Proces zpracování dat [1]

Z hlediska pojetí informace jako působení dat na změnu stavu nebo chování příjemce musí IS jako systém zpracování dat zabezpečit následující činností:

- vhodnou prezentaci potřebných dat pro příjemce ve vhodném čase,
- přenos dat určených pro prezentaci,
- zpracování prvotních dat na sekundární data určená k prezentaci,
- uchování dat určených pro zpracování,
- přenos primárních dat z místa pořízení na místo uchování,
- případné pořízení dalších primárních dat jejich převzetím z jiného IS.

Informační systém je principiálně technologicky nezávislý. Přenos dat lze tedy realizovat prostřednictvím informačních technologií nebo pomocí manuálního přemísťování záznamů.

2.1.2 Systém pravidel a způsobů řízení v určité organizaci

Pokud IS vnímáme jako systém pravidel, předpisů a způsobů řízení v určité organizaci (včetně pravidelných porad a setkání vedoucích či řadových pracovníků), zdůrazňujeme u IS hledisko řízení.

2.1.3 Informační systém jako jeden ze systémů v každé organizaci

V tomto pojetí jsou často zdůrazňovány aktivity informačních technologií, jako obslužné aktivity zabezpečující hlavní činnost organizace.

2.1.4 Informační systém jako systém zahrnující aspekty více disciplín

Informační systém můžeme také považovat za systém zahrnující aspekty více disciplín (datových, organizačních, metodických, procesních, technologických, ekonomických a obchodně podnikatelských), jelikož hlavní otázkou je, jaké informace jsou potřebné pro úspěšný rozvoj prosperující společnosti. [1]

2.2 Veřejná správa

Veřejnou správou rozumíme správní činnost, která souvisí s poskytováním správních veřejných služeb a řízením veřejných záležitostí na místní i centrální úrovni. Za veřejnou správu bývají označováni též správní orgány, tedy především úřady. Veřejnou správu dělíme na státní správu a samosprávu.

Funkce veřejné správy:

- **mocenská** - je realizována pomocí právního řádu a působením státního zřízení,
- **bezpečnostní** - zahrnuje povinnost zajistit vnitřní a vnější bezpečnost státu,
- **organizační** - spočívá v organizaci státních záležitostí a občanských záležitostí,
- **ekonomicko-regulační** - zabývá se usměrňováním vývoje ekonomiky,
- **služba veřejnosti** - jedná se o činnosti poskytované výhradně ve veřejném zájmu. [3]

V širším pojetí je veřejná správa představována mocí veřejnou, zákonodárnou a výkonnou. Moc zákonodárná je představována parlamentem, moc výkonná prezidentem, vládou a správními úřady, moc soudní poté samotnými soudy.

Veřejnou správu členíme do dvou směrů. V první řadě jako určitou veřejnou činnost (tzv. funkční pojetí veřejné správy) a dále jako soustavu orgánů (subjektů), které tuto činnost vykonávají (tzv. organizační či institucionální pojetí veřejné správy).

Činnost veřejné správy může mít též několik podob. Hovoříme o tzv. vrchnostenské (výsostné) veřejné správě, kde jde o činnost nařizovací (autoritativní), která má povahu veřejné moci. Orgán veřejné moci (např. orgán obce) v tomto případě zasahuje do právních poměrů jiných osob (fyzických nebo právnických). Pro vrchnostenskou veřejnou správu je

typická existence vztahů nadřízenosti a podřízenosti, ve kterých orgán veřejné správy vždy stojí výše nad osobou, o jejichž právech nebo povinnostech rozhoduje. Výstupem vrchnostenské veřejné správy jsou správní rozhodnutí vydaná ve správním řízení, ale i další úkony správních orgánů, které zasahují do práv a povinností adresátů veřejné správy (např., veřejnoprávní smlouvy, osvědčení nejrůznějšího typu aj.).

Další formou činnosti veřejné správy je činnost nevrchnostenská (nevýsostná, fiskální) spočívající v zajišťování určitých veřejných potřeb. Jedná se o pečovatelskou či obhospodařovací činnost. Pro tuto činnost jsou typické naopak rovnoprávné vztahy mezi orgány veřejné správy a jejími adresáty (např. správa státního majetku). Při nevrchnostenské veřejné správě vstupují orgány veřejné správy do soukromoprávních vztahů (např. občanskoprávních). [4]

2.3 Informační systém veřejné správy

Informační systém veřejné správy tvoří soubor informačních systémů, které jsou určeny k výkonu veřejné správy. [1]

Správcem informačního systému veřejné správy (ISVS) je osoba, která je odpovědná za ISVS a určuje účel informačního systému, jaké informace bude evidovat a zpracovávat a pomocích jakých prostředků budou tyto informace poskytovány jiným informačním systémům veřejné správy.

Provozovatel informačního systému je naopak osoba, která má na starost provoz informačního systému veřejné správy. Tato osoba má za povinnost provádět alespoň některé informační činnosti spojené s činnostmi ISVS. K těmto činnostem patří zejména získávání a poskytování informací, shromažďování, vyhodnocování a ukládání dat na hmotné nosiče, uchovávání, vyhledávání, úprava nebo změna dat. Dále sem patří šíření těchto dat, předávání, zpřístupnění, výměna, třídění a likvidace dat uložených na hmotných nosičích.

Rozdíl mezi správcem a provozovatelem je tedy určující v rozsahu jejich odpovědnosti. Správce obdobně jako provozovatel poskytuje informační služby, nicméně je za ISVS plně odpovědný. Správce i provozovatel ISVS jsou povinni dodržovat příslušné standardy. Správci ISVS mohou být ministerstva, správní úřady, orgány územní samosprávy a další orgány veřejné správy. [5]

2.4 Životní cyklus vývoje informačních systémů veřejné správy

2.4.1 Příprava informačního systému

Při přípravě ISVS musí nejprve správce IS vyplnit dokument Záměr informačního systému _ Evidenční list. Potřebu pro vytvoření IS musí správce důkladně zdůvodnit. Správce vypracuje informační strategii systému, vymezí a analyzuje požadavky na informační systém, provede analýzu výchozího stavu a pro rozvoj IS a určí cílový stav IS. Dále definuje postupy řízení bezpečnosti, plánování, řízení projektů, monitorování a aktualizace požadavků na IS a řízení jakosti. Správce IS je povinen zpracovat dokumenty Bezpečnostní politika, Plán zajištění jakosti, Principy monitorování a aktualizace požadavků a Projektové postupy. [1]

2.4.2 Vývoj, provoz a údržba informačního systému

Tato fáze se týká aktualizace informační strategie. Při vývoji, provozu a údržbě IS jsou uplatňovány zásady bezpečnosti celého IS. Tyto zásady IS musí být v souladu s bezpečnostní politikou společnosti. Správce IS také aktualizuje dokumenty Informační strategie, Bezpečnostní politika, Projektové postupy, Plán zajištění jakosti, Principy monitorování a aktualizace požadavků a Systémové požadavky. Pro tuto fázi jsou typické realizační projekty, které rozdělujeme do šesti základních skupin:

1. **Projekty akvizice** – zde se jedná o získání IS od externího dodavatele.
2. **Projekty vývoje** – vývoj samotného IS nebo jeho části, softwarové produkty nebo služby, softwarové produkty nebo služby nad rámec běžné údržby IS, modifikace IS nebo jeho části. U projektů vývoje probíhá analýza požadavků, návrh, programování, testování, instalace a převzetí IS.
3. **Projekty redukovaného postupu vývoje** – tento postup vývoje se používá pro projekty, které nevyžadují změnu právních předpisů, mají omezené nebo téměř žádné vazby na jiné systémy veřejné správy a pro projekty s jednoduchou strukturou.
4. **Projekty základního postupu vývoje** – základní postup vývoje se používá pro ostatní projekty, které nesplňují požadavky redukovaného postupu vývoje.
5. **Projekty provozu a údržby –** zabývají se provozem celého IS či jeho části. Projekty řeší provozní podporu uživatelů, drobné opravy IS, které nemění jeho funkčnost, přechod systému na novou verzi, kdy se rovněž nemění funkčnost systému.

6. **Kombinované projekty –** jedná se o kombinaci dvou a více projektů výše uvedených. [1]

2.4.3 Ukončení činnosti informačního systému

Jde o konečné vyřazení informačního systému z provozu bez náhrady. O vyřazení ISVS musí správce vyplnit Protokol o vyřazení informačního systému z provozu _ Evidenční list.

Všechny dokumenty musí správce IS schválit, o schválení provede zápis, jenž je součástí dokumentu. Dokumenty archivuje správce po dobu pěti let od ukončení provozu IS, pouze Evidenční listy se zasílají na příslušné ministerstvo. [1]

2.5 Klasifikace informačních systémů veřejné správy

Informační systém veřejné správy rozdělujeme dle různých kritérií. K nejčastějším z nich řadíme členění IS podle typu řízení, územního hlediska, předmětové oblasti, typu používané softwarové aplikace a dle jednotlivých oblastí veřejné správy.

2.5.1 Informační systém podle typu řízení

Informační systémy dle typu řízení dělíme do dvou základních kategorií:

1. Informační systémy pro státní správu
2. Informační systémy pro územní samosprávu

U informačních systémů na úrovni měst a obcí je problematické určit přesnou hranici mezi těmito druhy sytému. Městské i obecní úřady vykonávají jak činnost státní správy, tak činnost územní samosprávy, které jsou vedeny ve stejném informačním systému města nebo obce.

2.5.2 Informační systém dle územního hlediska

Na nejnižší, lokální úrovni existují informační systémy měst a obcí. Na vyšší, regionální úrovni existují informační systémy krajů. Samostatným informačním systémem je IS hlavního města Prahy.

2.5.3 Informační systém podle předmětové části

Z důvodu velkého množství různých typů organizací v oblasti veřejné správy existují také různé druhy informačních systémů. Podle tohoto hlediska rozeznáváme:

- Informační systémy jednotlivých ministerstev (rezortní informační systémy)
- Informační systémy organizací veřejné správy (nevýdělečné organizace, příspěvkové organizace a jiné typy organizací)
- Specializované systémy (evidence nemovitostí, kartotéky, geografické informační systémy)

2.5.4 Informační systém podle typu používané softwarové aplikace

Jedná se zde o konkrétní programové produkty, které jsou používány jednotlivými organizacemi a institucemi veřejné správy. Vážným problémem je zde kompatibilita těchto systémů. V mnoha případech neexistují žádné vazby na další informační systémy.

2.5.5 Informační systém dle jednotlivých oblastí

Existují informační systémy úřadů práce, zdravotních pojišťoven, finančních úřadů, institucí sociálního zabezpečení a dalších typů organizací. K ISVS řadíme i veřejné informační služby – informační systémy knihoven, muzeí, archívů a informačních středisek. [1]

3 PRÁVNÍ ÚPRAVA A NORMY

Problematika nakládání s informacemi začíná na úrovni státu. Česká republika řeší tuto oblast právními předpisy, které jsou zveřejněny ve sbírce zákonů.

3.1 Právní předpisy

- zákon č. **101/2000** Sb., o ochraně osobních údajů a změně některých zákonů,
- zákon č. **499/2004** Sb., o archivnictví a spisové službě a o změně některých zákonů,
- zákon č. **227/2000** Sb., o elektronickém podpisu a o změně některých dalších zákonů,
- zákon č. **412/2005** Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,
- zákon č. **240/2000** Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). [2]

3.2 Zákon č. 365/2000 Sb., o informačních systémech veřejné správy

Informační systém veřejné správy se řídí zákonem č. **365/2000** Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. V tomto zákoně jsou také uvedeny definice základních pojmů v oblasti ISVS. [1]

„Zákon o informačních systémech veřejné správy stanoví práva a povinnosti správců informačních systémů veřejné správy (ISVS) a dalších subjektů, jež souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. V návaznosti na to upravuje působnost Ministerstva vnitra jako ústředního správního úřadu pro tvorbu a rozvoj informačních systémů veřejné správy. Zákon vytváří podmínky, aby kvalitní informační systémy byly dobrým nástrojem pro výkon veřejné správy.“

„Zákon dále mj. upravuje atestace a postavení atestačních středisek, doručování zpráv orgánům veřejné moci prostřednictvím portálu veřejné správy a poskytování ověřených výstupů z ISVS.“ [6]

Zákon o ISVS se nevztahuje na informační systémy veřejné správy vedené zpravodajskými službami, Policií České republiky při plnění jejich úkolů, Ministerstvem financí, Národním bezpečnostním úřadem aj. Ústřední funkci zde zastupuje Ministerstvo vnitra. Vyhledává a zpracovává nové informace, které tvoří základ pro tvorbu a rozvoj informačních systémů veřejné správy. Orgány veřejné správy, jakožto tvůrci informační koncepce, popisují

v tomto dokumentu své dlouhodobé cíle v oblasti řízení kvality a bezpečnosti ISVS, dále jejich uplatnění a následné vyhodnocení dodržovaných postupů v praxi. Dále se zde určuje prováděcí právní předpis s přesně stanoveným obsahem a strukturou, ve kterém je uvedena provozní dokumentace k jednotlivým ISVS. Orgány veřejné správy jsou povinny zajistit atestaci dlouhodobého řízení ISVS a prokázat tak splnění stanovených podmínek dle zákona. Rozsah provozní dokumentace je rovněž stanoven prováděcím právním předpisem. Orgány veřejné správy jsou dále odpovědné za vhodný výběr a zavedení přiměřených bezpečnostních opatření podle stanovených bezpečnostních požadavků.

V případě, že je při kontrole ministerstva u orgánu veřejné správy zjištěn nedostatek, je tento orgán vyzván k nápravě zjištěných nedostatků v předem dohodnuté lhůtě nepřesahující dobu 6 měsíců. Dalším důležitým krokem je provádění akreditace. Akreditaci provádí právnická osoba, která je členem mezinárodního sdružení a byla rozhodnutím ministerstva k této akci pověřena. Akreditující osoba je povinna postupovat v souladu s akreditačními pravidly.

Atestace, prováděné atestačními středisky, musí být v souladu s atestačními podmínkami. Během této činnosti je nezbytně nutné provádět posuzování dlouhodobého řízení ISVS a způsobilosti k realizaci vazeb ISVS s jinými informačními systémy za pomoci referenčního rozhraní. Referenčním rozhraní tvoří souhrn právních, organizačních, technických a dalších opatření vytvářejících jednotné integrační prostředí ISVS poskytující soustavu společných služeb určených k výměně oprávněně požadovaných informací mezi jednotlivými IS orgánů veřejné správy a dalšími subjekty. Cílem atestace referenčního rozhraní je posouzení, jestli je vazba realizovatelná. [7]

3.3 General data protection regulation (GDPR)

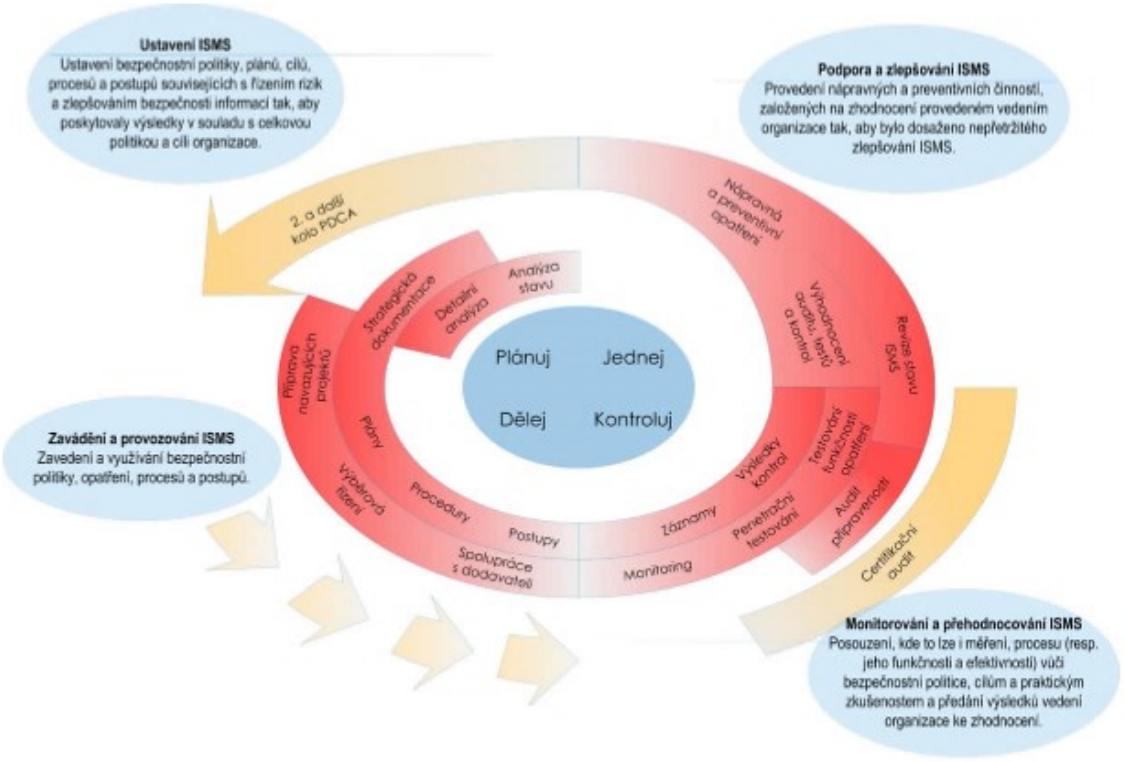
Dne 25. 5. 2018 vstoupí v platnost obecné nařízení o ochraně osobních údajů (GDPR), které plně nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů. Účelem směrnice Evropského parlamentu a Rady 2016/679 je harmonizovat právní předpisy o ochraně základních práv a svobod fyzických osob v souvislosti s činnostmi zpracování osobních dat a zajištění volného pohybu osobních údajů mezi členskými státy. Cílem GDPR bude tedy především posílení ochrany osobních údajů občanů v rámci celé Evropské unie. [8]

3.4 Systém řízení bezpečnosti informací (ISMS)

Systém řízení bezpečnosti informací je založený na mezinárodních normách ISO/IEC 27001 a ISO/IEC 27002. Je plně kompatibilní s řízením kvality dle ISO 9001, systémem environmentálního managementu dle ISO 14001, směrnicemi OECD (Organizace pro hospodářskou spolupráci a rozvoj). Tvoří ucelený popis bezpečnosti informací, je významným tvůrcem požadavků a vztahů na evropské úrovni. Představuje osvědčený způsob, jak zajistit a řídit bezpečnost informací a integrovat ji do stávajícího systému řízení organizace.

Cílem ISMS je aktivně řídit rizika, která pro organizaci vyplývají z využití informačních systémů a technologií a ze závislosti procesů na informacích.

ISMS prosazuje procesní přístup na základě Demingova cyklu Plánuj (Plan) – Dělej (Do) – Kontroluj (Check) – Jednej (Act). Tento model PDCA je aplikován na všechny procesy ISMS tak, jak jsou zavedeny normou ISO/IEC 27001. ISMS tvoří část celkového systému řízení organizace, je založen na přístupu k provozním rizikům, která se zaměřují na vybudování, zavádění, provoz, monitorování, přehodnocování, údržbu a zlepšování bezpečnosti informací. [9]



Obr. 2. PDCA model ISMS [9]

3.4.1 Norma ČSN ISO/IEC 27001 a 27002

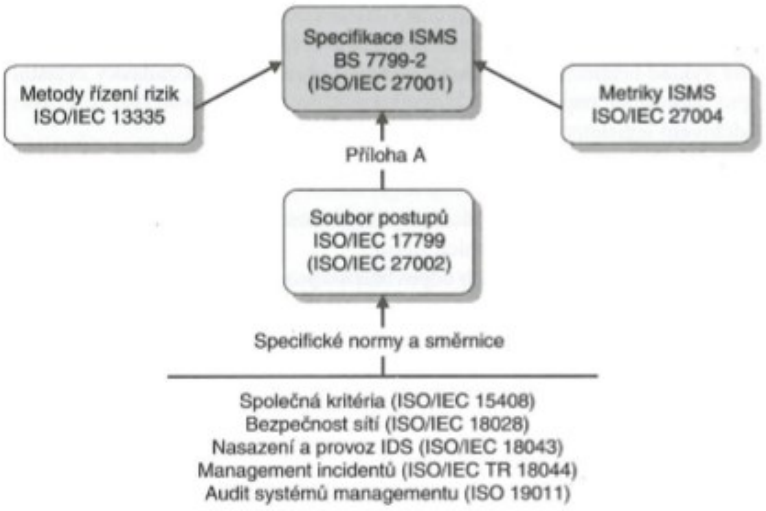
Norma ISO 27001 poskytuje model pro zavedení efektivního systému řízení bezpečnosti informací (ISMS) v organizaci a doplňuje tak normu ISO 27002. Obě normy jsou úzce propojeny, každá z nich však plní jinou roli. Zatímco norma ISO 27002 poskytuje podrobný přehled bezpečnostních opatření, které mohou být vybrány při budování ISMS, norma ISO 27001 specifikuje požadavky na to jak ISMS v organizaci správně zavést. Případná certifikace ISMS pak probíhá podle ISO 27001.

ISO/IEC 27001:2013

Norma ISO/IEC 27001 poskytuje model pro zavedení a správu efektivního systému řízení bezpečnosti informací. Norma stanovující jednoznačné požadavky na systém řízení, umožňuje kontrolu zavedení ISMS a případnou certifikaci, tedy nezávislé ověření ISMS třetím subjektem.

ISO/IEC 27002:2013

Toto vydání mezinárodní normy obsahuje více než 114 strukturovaných oblastí doporučení, která jsou rozdělena do 14 kapitol obsahující více než 5000 přímých a odvozených bezpečnostních opatření, podporujících dosahování podnikatelských cílů. Odpovědnost za tyto cíle je možné jednoduše přiřadit osobám s odpovídajícími funkcemi. To umožňuje velmi rychle zjistit stav bezpečnosti informačního systému organizace a zároveň vytvořit východiska pro jeho zlepšení, zejména pak vymezením oblastí, které nejsou dostatečně zajištěny. [10]

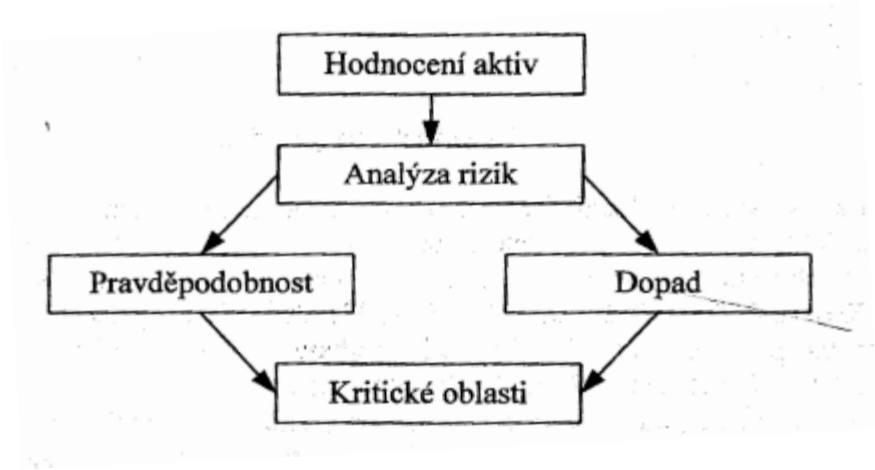


Obr. 3. Normy ze série ISO/IEC 27000 a další normy [11]

4 ANALÝZA RIZIK

Každá aktivita organizace je přímo spojena s podnikatelským rizikem. Toto riziko je definováno jako nebezpečí, že určitá událost negativně ovlivní schopnost dosahovat vytyčených cílů a strategií. Míra rizika je dána velikostí negativního dopadu a pravděpodobností s jakou toto riziko nastane.

V průběhu života organizace je nutné určitá rizika přijmout a řídit je. Tato činnost platí jak v podnikání, tak pro informační systémy. Cílem analýzy je identifikovat a kvantifikovat rizika, aby bylo možné rozhodnout o jejich přijatelnosti pro organizaci. Velikost rizika je dána pravděpodobností výskytu a dopadu pro organizaci. Tato analýza je pak využitelná pro informační systém organizace či společnosti. [1]



Obr. 4. Analýza rizik [1]

4.1 Analýza rizik informačního systému

Analýza rizik je důležitou aktivitou v oblasti bezpečnosti informačního systému, která musí odpovědět na následující otázky:

- Co se stane, když nebudou informace chráněny?
- Jak může být porušena bezpečnost informací?
- S jakou pravděpodobností se to stane?

Výstupem tohoto kroku se stává dokument obsahující popis systému a výsledky analýzy. Obsahuje úroveň hrozeb, identifikované zranitelnosti, úroveň stávajících ochranný opatření a šíření výsledných rizik. [12]

Jelikož podrobná analýza pro rozsáhlé informační systémy je časově náročná a informační rizika hrozícím organizacím nejsou tak vysoká, aby vyžadovala provedení podrobné analýzy, definuje ISO/IEC 13335 čtyři způsoby provádění analýzy rizik. Jedná se o tyto přístupy:

- základní přístup,
- neformální přístup,
- podrobná analýza rizik,
- kombinovaný přístup.

4.1.1 Základní přístup

Jedná se o metodu rychlého zavedení určitých bezpečnostních opatření bez podrobnější analýzy. Aplikovaná opatření jsou přijata z některého standardu v oblasti informační bezpečnosti. Výhodou je zde rychlost nasazení a minimální množství zdrojů pro analýzu rizik. Jedná se o úspornou metodu z důvodu užití standardních řešení. Nevýhodou je zde implementace sady opatření bez přizpůsobování úrovni rizika v jednotlivých případech. V některých oblastech tak mohou být opatření nedostatečná či příliš nákladná. Užití tohoto přístupu je vhodné u organizací s nižší úrovní bezpečnostních požadavků.

4.1.2 Neformální přístup

Tento přístup je zcela pragmatický. Není založen na předem definovaných metodologiích, ale vychází ze zkušeností jednotlivců a z daného prostředí. Výhodou je zde podstatná rychlost a nenákladnost.

4.1.3 Podrobná analýza rizik

Podrobná analýza rizik představuje nejpodrobnější a současně nejdražší metodu analýzy rizik. Jednotlivé kroky směřují od identifikace a ohodnocení aktiv a posouzení hrozeb pro tato aktiva až po odhad zranitelnosti. Takto zjištěné informace jsou poté použity k odhadu rizik a na základě odhadu rizik jsou dále identifikována bezpečností opatření. Jednotlivá bezpečností opatření jsou přizpůsobována úrovni zjištěných rizik.

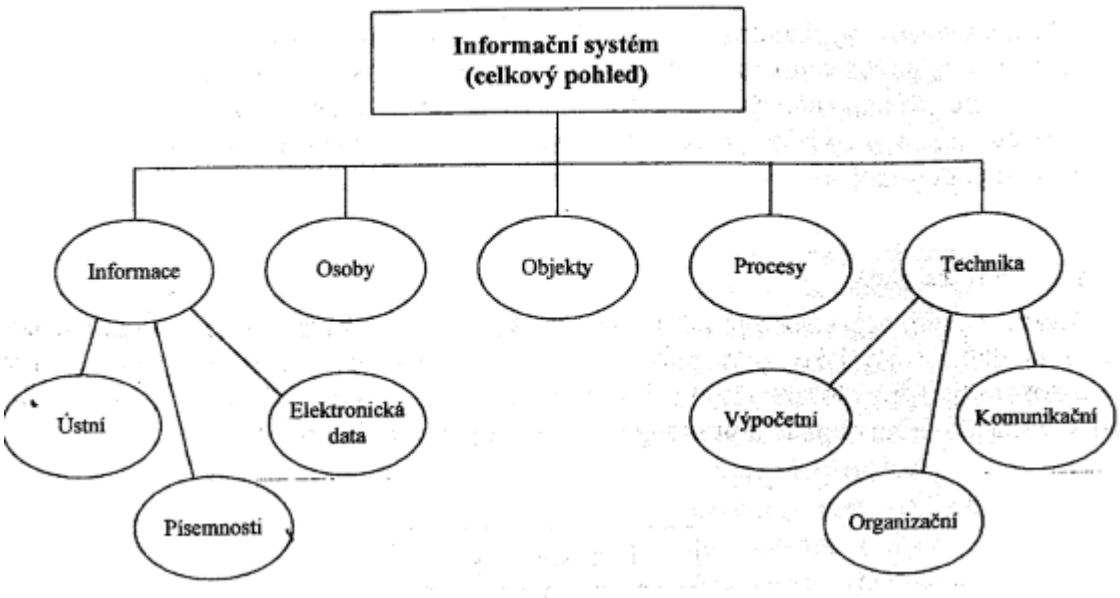
4.1.4 Kombinovaný přístup

Tento přístup se užívá k plánování analýzy rizik velké organizace kombinací základního přístupu a podrobné analýzy rizik. Umožňuje získat rychlý přehled o hrozících rizicích

pro informační systém a zároveň o rizicích, která hrozí kritickým součástem IS. Podrobnou analýzu je pak možné doplnit pro další části IS během delšího časového období.

Během analýzy rizik se mohou vyskytnout následující problémy či chyby:

- plošné zavádění ochranných opatření,
- nedostatečné využití analýzy rizik,
- neúplná analýza rizik,
- analýza rizik není aktualizována,
- subjektivní výběr protiopatření. [12]



Obr. 5. Rozsah analýzy rizik [1]

4.2 Bezpečnostní politika informačních systémů

Bezpečnostní politika informačního systému (BPIS) představuje dokument, který vychází z požadavků zákona č. 365/2000 Sb., o informačním systému veřejné správy (ISVS) a jeho prováděcí vyhlášky č. 529/2006 Sb., o dlouhodobém řízení ISVS. Bezpečnostní politika informačního systému je součástí provozní dokumentace ISVS. [13]

Cíle bezpečností politiky představují:

- definovat hlavní cíle při ochraně informací,
- stanovit způsob, jakým bezpečnost řešit,

- určit pravomoci a zodpovědnosti.

Bezpečnostní politika je tvořena souborem pravidel, norem a požadavků, které formulují přístup daného subjektu k zajištění integrity, dostupnosti informací a důvěrnosti. Obsahuje souhrn bezpečnostních požadavků určených k řešení informační bezpečnosti na úrovni administrativní, fyzické a datové. [14]

Bezpečnostní politika IS definuje výstupy pro další kroky společnosti v oblasti informační bezpečnosti. Z požadavků kladených na politiku automaticky nevyplývá úroveň detailu a jeho rozsah. Dle rozsahu rozpoznáváme stručný a rozsáhlý dokument. Stručný dokument obsahuje definice základních principů, odpovědností a pravomocí. Rozsáhlý dokument pak řeší oblast úrovně podrobnosti normálního řešení pomocí standardů.

Po vytvoření bezpečnostní politiky je nezbytně nutné seznámit s tímto dokumentem všechny zaměstnance. V případě rozsáhlejších politik není nutné seznámit zaměstnancem s celým dokumentem, ale pouze s částmi, které bezprostředně souvisí s výkonem jejich pracovních funkcí.

4.2.1 Problémy a chyby vyskytující se při tvorbě politiky

Při tvorbě bezpečnostní politiky může dojít k následujícím problémům či chybám:

- velké množství kompromisů,
- nereální bezpečnostní politika,
- neadekvátní rozsah politiky,
- podcenění propagace politiky,
- nekritické přebírání vzorců. [12]

5 ZRANITELNOST INFORMAČNÍHO SYSTÉMU

Zranitelnost je obecnou vlastností informačních systémů. Můžeme ji posuzovat ze dvou hledisek: z hlediska organizačního a logického prostředí. Jedná se o lidské zdroje a samotné technické zdroje (hardware i software). Zranitelnost infomačního systému je dána mírou rizika, jež se rovná pravděpodobnosti uplatnění některých ze zranitelných nebo obecných rizik. Nejpravděpodobnější hrozba pramení z hrozby organizačního prostředí. Systém je buď dodán, instalován nebo používán způsobem, který není bezpečný. [15]

5.1 Uživatelé

Jednu z hrozeb organizace tvoří i její vlastní zaměstnanci. Mohou je vést různé motivy, mezi nejčastější důvody patří:

- nespokojenost zaměstnance s platem či pracovním zařazením,
- zloba na zaměstnavatele či jiné zaměstnance,
- škodolibost, pomstychtivost či závist a další.

Rozšířením přístupů a práv získává zaměstnanec více možností k neoprávněným úkonům a organizaci hrozí tak ztráta dat či informací nebo jejich zneužití. [16]

Společnost by si měla v každém případě dávat pozor na to, jaké lidí zaměstnává. Po ukončení pracovního poměru je nezbytně nutné okamžitě zablokovat všechna práva zaměstnance do systému a tím tak předcházet ke ztrátě či zničení dat. [17]

5.2 Útoky hackerů

Termín hacker představuje osobu, která je svými schopnostmi a dovednosti v oblasti informační technologie schopna získat neoprávněný přístup k počítačům. Podstatou tohoto jednání je získat hesla uživatelů nebo vytvoření vlastního programu, který je schopen obejít bezpečnostní software chránící počítač. Způsob, jak se útokům hackerů ubránit, je pravidelná bezpečnostní aktualizace programů. Hackerské nástroje, jsou navrženy takovým způsobem, aby pomáhali hackerovi v jeho činnosti. Právě za pomoci škodlivého softwaru jako je počítačový vir či trojský kůň je hacker schopen získat neoprávněným přístupem požadovaná hesla. Rozeznáváme několik druhů hackerů dle jejich záměrů a cílů. [17]

5.3 Viry a škodlivý software

Škodlivý software, známý pod pojmem malware, je každý software, který nějakým způsobem škodí počítačovému systému. Malware může být ve formě virů, červů, trojských koní, atd., které kradou chráněná data, smazávají dokumenty nebo přidávají software neschválený uživatelem. [18]

5.3.1 Počítačový vir

Počítačový virem se označuje počítačový program, který patří do oblasti malwaru. Počítačový vir má s biologickým virem velmi podobné vlastnosti, a právě proto převzal toto pojmenování. Vir v sobě obsahuje škodlivý kód a šíří ho dále vkládáním do dalších souborů například zasláním po síti či pomocí disku. [19]

Kromě samotné reprodukce může kód viru vykonávat různé grafické, zvukové a textové efekty, dále pak i činnosti destrukčního rázu jako je mazání, kódování a jiné modifikace souborů. Viry mají schopnost narušit bezpečnost počítače zasíláním tajných PGP (Pretty Good Privacy) klíčů, odchycených hesel a e-mailových adres. [20]

Počítačové viry dělíme do několika skupin podle toho, jaké objekty napadají:

- **Boot viry** - napadají systémové oblasti disku. Šíří se následovně: v případě restartování počítače, který má povolen zavádět systém z disketové mechaniky a v mechanice je disketa s boot virem, vir se spustí a napadne systémové oblasti pevného disku. Při spuštění počítače dochází k instalaci boot viru z pevného disku a napadení diskety, kterou uživatel použije. V praxi se tyto typy virů vyskytují častěji než viry souborové.
- **Souborové viry** - napadají pouze soubory, které obsahují prováděný kód - programy. V napadeném programu změní část kódu svým vlastním, nebo připojí vlastní kód k programu a tím změní jeho chování a velikost.
- **Multipartitní viry** - napadají soubory i systémové oblasti disku. Kombinují boot viry se souborovými.
- **Makroviry** - napadají datové soubory (dokumenty vytvořené v kancelářských aplikacích). Využívají toho, že tyto soubory neobsahují pouze data, ale i makra, která využívají viry ke svému šíření. Jedná se zejména o dokumenty aplikací MS Office. Makroviry jsou v současnosti nejčastěji se vyskytujícím druhem viru. Představují nejfatálnější hrozbu do budoucna.

- **Stealth viry -** jedná se o viry, které se chrání před antivirovým programem užitím stealth technik. Pokud je takový virus v paměti, pokouší se přebrat kontrolu nad některými funkcemi operačního systému a při pokusu o čtení infikovaných objektů vrací hodnoty odpovídající původnímu stavu.
- **Polymorfní viry –** snaží se zkomplikovat své odhalení tím, že změní vlastní kód. V napadeném souboru není možné najít typické sekvence stejného kódu.
- **Rezidentní viry -** po svém spuštění zůstávají i nadále přítomny v paměti. [21]

5.3.2 Červ

Počítačovým červem rozumíme počítačový program, který je schopen zasílat kopie sebe sama na další počítače a tím tak převezme kontrolu nad infikovaným systémem. Kromě svého vlastního šíření vykonává červ v počítači nějakou sekundární činnost, která spočívá v následujících činnostech:

- ukončení provozu počítače nebo jeho části,
- odstranění souborů uložených v počítači,
- prohledávání počítače za účelem získání osobních dat,
- vytváření tzv. zadních vrátek (backdoor) do systému, která jsou poté využita k infikaci počítače aj. [22]

5.3.3 Trojský kůň

„Trojským koněm rozumíme program, který navenek navozuje dojem užitečnosti, v dokumentaci programu slibovanou činnost však buď vůbec nevykonává, nebo ji vykonává, ale v pozadí realizuje nepozorovaně nějaký druh destrukce (maže soubory, formátuje pevný disk, skrytou komunikací přes internet narušuje soukromí uživatele a podobně).“ [23]

Trojský kůň může být naprogramován jako původní aplikace nebo naopak vytvořen z již existujícího programu spojením s destrukčním kódem. Takto vytvořený program se od původního programu kromě délky navenek ničím neodlišuje. [20]

Obvykle jsou tyto programy určeny ke krádeži osobních údajů, šíření jiných virů nebo ke snížení výkonnosti počítače. Kromě toho jej mohou hackeři využit k získání neoprávněného vzdáleného přístupu k ohroženému počítači, infikovat obsažená data a celkově poškodit systém. Jakmile se trojský kůň dostane do počítače, začne se před obětí schovávat. Trojské koně jsou obdobné běžným virům, a proto je jejich odhalení nelehké.

Činnosti způsobené trojským koněm:

- infikovat, poškodit, přepsat nebo zničit celý systém smazáním kritických souborů nebo formátováním pevných disků,
- sledovat uživatele a každý jeho úhoz na klávesnici,
- instalovat backdoor nebo aktivovat vlastní komponenty využitelné pro následnou činnost útočníka,
- blokovat uživatelům přístup ke spolehlivým internetovým stránkám aj. [24]

5.3.4 HOAX

Hoax, v anglickém překladu falešná zpráva, představuje e-mailovou zprávu, která obsahuje nepravdivé upozornění o nákaze novým tipem viru, případně jinou falešnou informaci, kterou uživatelé dále rozšiřují po síti mezi své přátele na co největší množství adres. Často bývá tvrzení pisatele doprovázeno velmi expresivními obrázky (nádory, tělesná postižení, oběti autonehody, nebezpečných zvířat). [25]

Hoaxy jsou často označovány za tzv. urban legends (městské legendy), které nejsou stavěny na pevném základu. Jsou tvořeny tak, aby jim bylo možné lehce uvěřit a aby uživatel neměl zájem ověřit pravdivost informace.

Negativní vlivy hoaxu:

- **Obtěžování příjemců** - hoaxy velmi často obtěžují příjemce, jejichž e-mailovou schránku zaplaví. Zejména v době epidemie se v e-mailové schránce příjemce objevuje stejná zpráva i několikrát denně.
- **Nebezpečné rady** - hoaxy mohou i poskytnout nebezpečné rady, např. jak se zbavit domnělého viru smazáním nějakého souboru. Uživatel, který na tyto rady dá, může svému počítači naopak ublížit.
- **Nadbytečné zatěžování linek a serverů** - řada hoaxů se šíří ve statisícových kopiích po celém světě, mohou tedy snadno přetěžovat linky i poštovní servery. Z tohoto důvodu bývají servery zabezpečeny anti-spamovými programy, které jsou dnes součástí každé kvalitní online mailové služby.
- **Ztráta důvěryhodnosti šiřitele** - odesílatel falešných zpráv ohrožuje svou důvěryhodnost, obzvláště pokud takové zprávy odesílá z pracovního e-mailu. V takovém případě může utrpět i pověst příslušné firmy nebo úřadu.

- **Prozrazení důvěrných informací** – v případě, že uživatel hoax přeposílá na mnoho dalších adres, často ponechá adresy všech příjemců ve zprávě, kde si je mohou všichni přečíst. Tímto způsobem se šíří objemný seznam e-mailových adres mezi předem neurčité množství cizích lidí a zvyšuje se tím možnost šíření spamu a počítačových virů. Spamy jsou úzce spjaty s pojmy phishing a pharming, v rámci kterých se útočník snaží získat různými způsoby osobní údaje uživatelů (rodné číslo, pin, hesla). [25]

5.4 Sociální inženýrství

Sociálním inženýrstvím je myšleno zneužívání lidské hlouposti či důvěřivosti s cílem manipulace a ovlivnění poškozeného za účelem získání požadovaných informací. Sociální inženýrství se dá definovat jako *„umění jak přimět ostatní lidi, aby splnili naše přání.“* Osoba sociotechnika se zaměřuje na selhání zaměstnance, dokáže využít jeho důvěřivosti a návyků. Pachatel si nejprve vytvoří průzkum v dostupných informačních zdrojích, kterými jsou webové stránky organizace, registry firem, výroční zprávy, reklamní materiály, e-mailové adresy zaměstnanců a jejich osobní údaje. Za pomocí sociálních sítí je poté pachatel schopen sledované osoby zkontaktovat a po krocích dosáhnout svých cílů. Celá akce je závislá na přesvědčovacích schopnostech a dovednostech útočníka. [17]

6 ZABEZPEČENÍ INFORMAČNÍHO SYSTÉMU

Informační systémy mohou být cílem působení nejrůznějších nebezpečí. Mohou to být lidé (vlastní zaměstnanci), události způsobené přírodními jevy (oheň, zásah bleskem, voda, zemětřesení, tsunami aj.), poruchy techniky (výpadky napájení, porucha zařízení). Lidské hrozby představují pak například teroristé, organizovaní zločinci, průmysloví agenti aj.

Fyzická poškození způsobená přírodními katastrofami a závadami zjistíme zpravidla ihned. Informační systém přestane být funkční a způsobené škody můžeme identifikovat. Při nelegálním úniku informací však nastává horší situace. Pokud nejsou získané informace použity, nelze téměř nic s jistotou dokázat. Většina útoků tak zůstane neodhalena.

Informační systém se brání řadou opatření, ty mohou mít různé podoby:

- administrativní,
- personální,
- logické,
- datové,
- fyzické. [5]

6.1 Administrativní bezpečnost

Administrativní bezpečnost představuje ochranu utajovaných dokumentů obsahující utajované informace. Pro práci s těmito daty je nutné stanovit pevný řád a postupy, jak s těmito informacemi pracovat. Jedná se například o tyto činnosti:

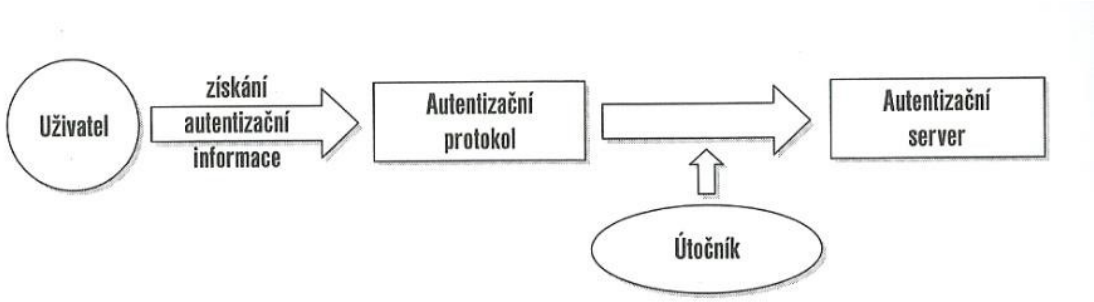
- příjem a zpracování informací,
- způsob jejich uložení,
- archivace, evidence a následná skartace. [1]

6.2 Personální bezpečnost

Tato bezpečnost spočívá v zajištění kvalifikovaného personálu, který bude mít na starost správu informačního systému. Zaměstnance organizace řadíme k nejrizikovějším faktorům podnikového bezpečnostního systému. Často se stává, že odpovědnost a spolehlivost personálu není na dostačující úrovni a dochází tak ke krádežím, podvodům a zneužití prostředků organizace. K předcházením těchto nežádoucích stavů je možno použít různých prověrek a testů prováděných na budoucích i současných zaměstnancích. [14]

6.3 Logická bezpečnost

Důležitou roli v oblasti logické bezpečnosti hraje operační systém. Pomocí operačního systému jsme schopni nastavit přístupová práva a ověřit tak identitu uživatelů. Po identifikaci uživatele, probíhá následná autentizace, kde dojde k ověření identity uživatele. Autentizaci rozeznáváme pomocí znalostí, vlastností nebo vlastnictví. K ověření identity uživatele slouží speciální autentizační protokol. Samotný systém pro řízení přístupu pak uživateli pevně stanový druh přístupu a přístup k povoleným datům. [18]



Obr. 6. Schéma činnosti autentizačního protokolu [18]

6.4 Datová bezpečnost

Datová bezpečnost obsahuje širokou škálu bezpečnostních opatření. Do této problematiky můžeme zahrnout oblast:

- šifrování,
- elektronický podpis,
- zálohování,
- aktualizace,
- hesla,
- antivirová ochrana,
- firewall.

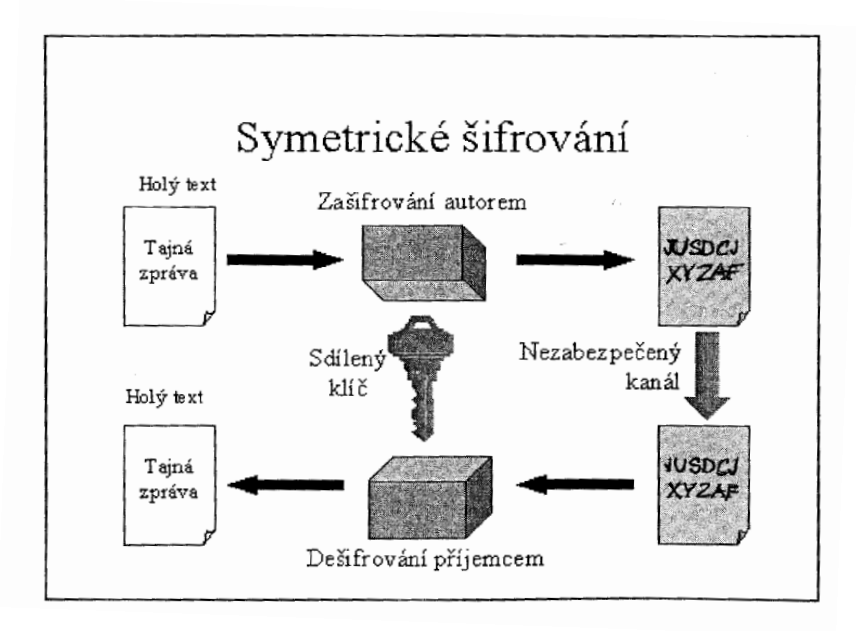
Šifrování

Kryptografií rozumíme vědu o šifrování dat za pomoci matematických metod. S tímto pojmem současně nesmíme opomenout i pojem kryptoanalýza, která se bez znalosti klíče snaží dojít k utajovaným datům. Kryptoanalýza je velmi náročná analytická metoda. Kryptografie a kryptoanalýza spolu tvoří obor, který nazýváme kryptologie. [5]

Kryptografie představuje transformaci dat do nečitelné podoby z důvodu ochrany důvěrnosti a integrity osobních dat. Kryptografické prostředky slouží nejen k zakrytí obsahu přenášených informací, ale také k bezpečnému doručení vyslané informace oprávněnému příjemci. Rozeznáváme dvojí tip šifrování:

- ***Symetrické šifrování***

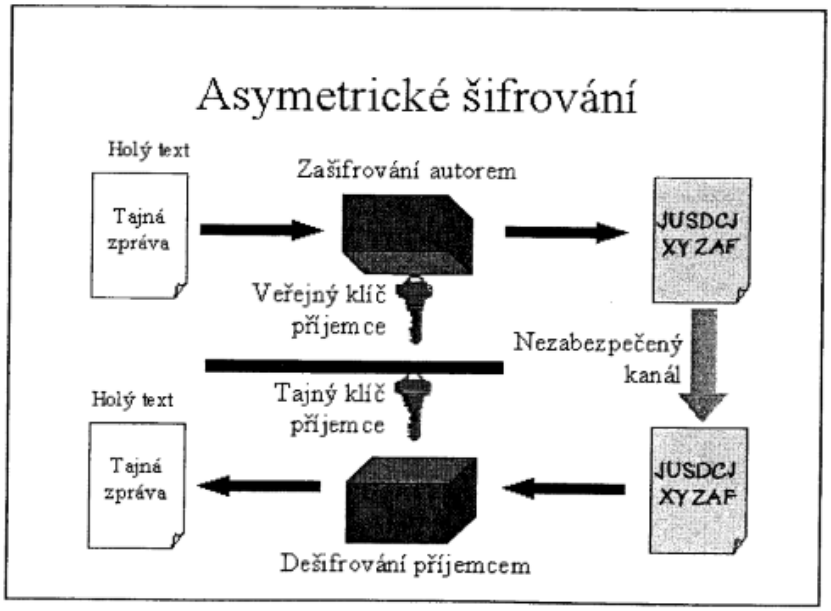
Symetrické šifrování užíváme k zabezpečení rychlého utajovaného přenosu většího objemu dat. U těchto šifer slouží jeden a ten samý klíč k šifrování i dešifrování dat. Symetrické šifry jsou tvořeny zejména prostřednictvím blokových šifer. Blokové šifry představují algoritmy zpracovávající otevřený text po větších blocích. Softwarová realizace těchto algoritmů zabezpečuje rychlé zašifrování objemného množství dat. [5]



Obr. 7. Princip symetrického šifrování [5]

- ***Asymetrické šifrování***

Při asymetrickém šifrování užíváme dva klíče. Veřejný klíč pro zašifrování zprávy (je přístupný komukoliv, kdo chce šifrovaně odeslat data příjemci zprávy) a soukromý klíč pro dešifrování. Soukromý klíč je tajný, a proto musí být střežen a chráněn. Ve skutečnosti se jedná o jeden klíč, který se při generování z počítačového programu rozdělí na dvě části, vzájemně neodvoditelné. Soukromý a veřejný klíč spolu tvoří klíčový pár. Neodvoditelnost klíčů a tedy dešifrování ze znalosti veřejného klíče vychází z matematických postupů, jejichž reverzní funkce je neproveditelná. [5]



Obr. 8. Princip asymetrického šifrování [5]

Elektronický podpis

„Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě“.

Elektronický podpis se užívá pro podepisování dokumentu libovolného obsahu a libovolné délky. Elektronický podpis má za úkol plnit následující funkce:

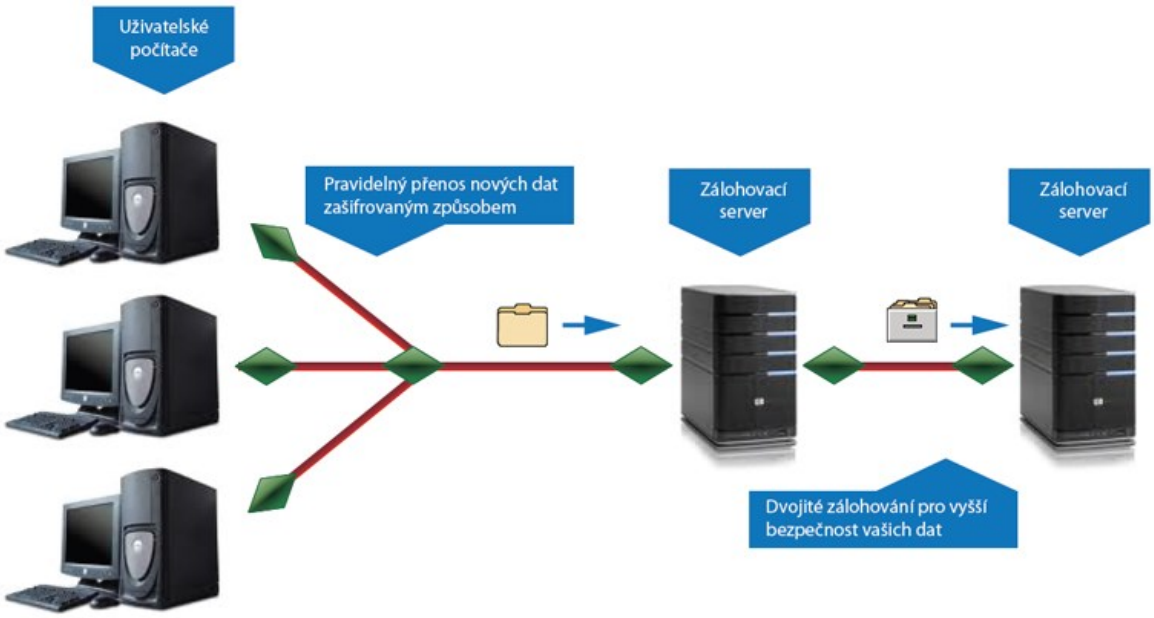
- identifikace (lze jednoznačně určit, kdo dokument podepsal),
- autentizace (lze zjistit, kdo je autorem daného dokumentu),
- integrita (znamená, že od vytvoření elektronického podpisu nebyl podepsaný dokument změněn ani poškozen),
- nepopiratelnost (autor podepsaného dokumentu nemůže popřít vytvoření dokumentu). [26]

Rozeznáváme elektronický podpis uznávaný a zaručený. Rozdíl spočívá v tom, že dokument s uznávaným elektronickým podpisem musí úřady akceptovat a dále s ním pracovat, jako s vlastnoručně podepsaným listinným dokumentem. Dokument, opatřený pouze zaručeným elektronickým podpisem, by naopak úřady uznávat neměly. Pokud jej přijmou, měly by se k němu chovat jako k nepodepsanému dokumentu. U zaručeného elektronického podpisu totiž lze údaj o podepsané osobě libovolně zfalšovat. [27]

Zálohování

Zálohování představuje proces, který umožňuje vytvořit kopii dat uchovávaných v zařízeních výpočetní techniky a uložit ji na další místo takovým způsobem, aby data byla dále dostupná v případě poškození nebo ztráty dat původních. Takto vytvořená kopie by neměla být uložena na stejném místě jako zdrojová data. [16]

Častou chybou při zálohování dat je uchovávání dat na běžných mediích jako jsou CD, DVD, flash paměti a podobně. Ztráta dat bývá v těchto případech způsobena mechanickým opotřebením média, jeho ztrátou nebo omezenou životností. Dalším nedostatkem je četnost takto prováděných záloh. Pravidelná a častá záloha dat tímto způsobem je velmi náročná a prakticky nereálná. V současné době roste zájem o zálohování dat pomocí internetu (vzdálené zálohování). [28]



Obr. 9. Grafické znázornění průběhu vzdálené zálohy [28]

Aktualizace

Pod pojmem aktualizace rozumíme určitý postup, při kterém je do počítače instalována novější verze programového vybavení (softwaru). Aktualizace bývá nejčastěji uskutečňována z důvodu zavedení vyšší bezpečnosti, oprav chyb nebo při přechodu na novější program. Pro tuto činnost se užívá i pojem patch (záplata). Velikost aktualizace bývá velmi různorodá. Závisí na tom, zda jsou aktualizovány celé soubory nebo pouze jeho části. V minulosti byly aktualizace prováděny pomocí děrných pásků, štítků a následně magne-

tických pásků. V současné době jsou aktualizace v největší míře prováděny pomocí internetu. [29]

Hesla

Hesla řadíme k nejdůležitějším prvkům bezpečnostního systému. Heslo představuje obranný prvek proti počítačové kriminalitě. Nejdůležitějším krokem je zvolit si odpovídající sílu hesla, kterou tvoří jeho délka a užití znaků. Čím delší a složitější heslo bude, tím bude doba prolomení delší. Přidání čísel, malých i velkých znaků a symbolů ztíží potencionálním útočníkům heslo uhodnout. Nedoporučuje se též užívat stejné heslo pro více účtů, ale vytvořit vždy nové. Důraz je kladen též na pravidelnou aktualizaci hesel. [30]

Antivirová ochrana

Stejně tak jako pravidelné zálohování dat je v dnešní době velmi důležitá ochrana před škodlivým softwarem (viry, červy aj.) formou antivirového programu. S užitím je důležité začít ihned po instalaci počítače nebo jeho prvním spuštění doinstalovat antivirový program, v případě, že ho neobsahuje. Pokud je součástí nového počítače i operační systém a antivirový program, je nutné provést jeho okamžitou aktualizaci. Po zapnutí a aktualizaci antivirového programu je teprve možné začít s následnou instalací dalších potřebných programů. Na trhu jsou dostupné komerční antivirové programy, za něž se platí, nebo programy určené pro domácí použití, které mohou být zdarma. [31]

Firewall

„Firewall je používán jako generický název pro všechna řešení, která mají za cíl zabezpečovat připojenou privátní síť před veřejným Internetem, zejména pak chránit ji před takovým druhem přístupu, jaký provozovatel privátní sítě považuje za nežádoucí“. [5]

Firewall představuje systém, který pomáhá zabránit škodlivému softwaru, virům nebo hackerům proniknout do počítače. To všechno se může dít prostřednictví internetu či sítě. Firewall také slouží k tomu, aby zabránil v odesílání škodlivého softwaru do jiných počítačů. Windows Firewall tvoří velmi kvalitní, spolehlivý a snadno nastavitelný paketový filtr. Firewall lze rozšířit i na menší sítě a to díky funkci sdíleného připojení. Stavy firewallu mohou být následující:

- **zapnuto** – v případě zapnutého firewallu dochází k blokaci komunikace u většiny programů, u požadovaného programu však můžeme přidat výjimku,

- **vypnuto** – není doporučováno, je možné ho použít, pokud uživatel není připojen k internetu,
- **blokovat všechna příchozí připojení** – zpravidla užíváno pro zajištění maximálního zabezpečení, není brán ohled ani na seznam přidaných výjimek. [32]

6.5 Fyzická bezpečnost

Cílem fyzické bezpečnosti je ochrana aktiv společnosti, budov, počítačů a médií před fyzickými útoky, které by mohli zapříčinit odcizení či znehodnocení těchto aktiv. Hlavním úkolem je zabránění přístupu nepovolených osob do prostor objektu. Fyzická bezpečnost zahrnuje ochranu objektu a jejich vnitřních prostor pomocí technologických zabezpečovacích prostředků a monitorovacích zařízení. Aktivní prvek této ochrany tvoří fyzické bariéry ve formě bezpečnostních perimerií - např. zdi, mříže aj. Míra zabezpečení by měla odpovídat zjištěným rizikům. [33]

II. PRAKTICKÁ ČÁST

7 PŘEDSTAVENÍ ÚŘADU PRÁCE

Úřad práce (ÚP) pod záštitou Ministerstva práce a sociálních věcí (MPSV) je organizačně členěn na generální ředitelství a krajské pobočky. Působení krajských poboček je shodné s územím jednotlivých krajů dle zákona č. 347/1997 Sb., o vytvoření vyšších územních samosprávních celků, ve znění pozdějších předpisů. Prvotním úřadem práce byl úřad práce v Kladně, který zahájil svou činnost v roce 1990.

Úřad práce ČR se člení na 14 krajských poboček, které jsou složeny z kontaktních pracovišť (KoP). Krajské pobočky z hlediska věcného zajišťují především nástroje aktivní politiky zaměstnanosti. Kontaktní pracoviště pak zajišťují agendy zprostředkování zaměstnání a státní sociální podpory. [34]

7.1 Politika zaměstnanosti

Náplní úřadu práce v oblasti politiky zaměstnanosti je zejména poskytování služeb spojených se zprostředkováním vhodného zaměstnání uchazečům o zaměstnání (UoZ), vyplácení podpory v nezaměstnanosti a podpory při rekvalifikaci. Dále uděluje cizincům povolení k zaměstnání v České republice. Poskytuje též poradenské služby v oblasti volby povolání, rekvalifikace či další možnosti vzdělávání. Osobám se zdravotním postižením zabezpečuje například pracovní rehabilitaci.

V rámci aktivní politiky zaměstnanosti může úřad práce poskytnout žadateli příspěvek na vytvoření pracovních příležitostí v rámci veřejně prospěšných prací nebo společensky účelného pracovního místa, dále příspěvek pro začínající podnikatele či poskytnout podporu na vytvoření chráněné pracovní dílny pro osoby se zdravotním postižením z prostředků Evropského sociálního fondu (ESF).

V níže uvedené tabulce je uvedena statistika nezaměstnanosti za období ode dne 1. 3. 2017 do 31. 3. 2018 rozčleněna na okres Hodonín, kontaktní pracoviště Kyjov, Jihomoravský kraj a stát. [35]

Tab. 1. Statistika nezaměstnanosti [36]

	Okres Hodonín			KoP Kyjov		JM kraj	ČR
	Počet UoZ na 1 volné místo	Počet UoZ	PNO (%)	Počet UoZ	PNO (%)	PNO (%)	PNO (%)
31.03.2017	7,1	7 985	7,4	2 359	6,7	5,7	4,8
30.04.2017	6,4	7 195	6,7	2 115	6,0	5,2	4,4
31.05.2017	5,0	6 607	6,2	1 933	5,5	4,8	4,1
30.06.2017	5,1	6 304	5,9	1 846	5,3	4,7	4,0
31.07.2017	5,0	6 328	5,9	1 883	5,2	4,8	4,1
31.08.2017	4,1	6 299	5,9	1 841	5,1	4,7	4,0
30.09.2017	3,6	6 090	5,7	1 789	4,9	4,5	3,8
31.10.2017	3,7	5 931	5,5	1 761	4,9	4,3	3,6
30.11.2017	3,6	5 855	5,5	1 751	4,9	4,3	3,5
31.12.2017	4,8	6 576	6,2	1 934	5,5	4,6	3,8
31.01.2018	4,2	6 884	6,4	1 999	5,6	4,8	3,9
28.02.2018	3,9	6 706	6,2	1 924	5,5	4,6	3,7
31.03.2018	3,1	6 182	5,7	1 776		4,3	3,5

7.2 Politika státní sociální podpory

Pod pojmem státní sociální podpory (dále jen SSP) označujeme dávky poskytované osobám ve společensky uznaných sociálních situacích, kdy stát skrze jejich vyplácení z části přebírá zodpovědnost za vzniklou sociální situaci. V rámci systému státní sociální podpory je poskytován přídavek na dítě, rodičovský příspěvek, sociální příplatek, příspěvek na bydlení, porodné, pohřebné a dávky pěstounské péče.

7.3 Fyzické uspořádání kontaktního pracoviště v Kyjově

Kontaktní pracoviště v Kyjově je rozděleno do dvou samostatných budov, z nichž v první z nich sídlí oddělení státní sociální podpory, v druhé pak oddělení zaměstnanosti, evidence a podpor v nezaměstnanosti, které bude předmětem dalšího popisu.

Pracoviště zaměstnanosti se nachází v druhém podlaží budovy České pošty v Kyjově se samostatným vchodem do prostor úřadu práce. Objekt se skládá z desíti kanceláří, sociálního zařízení pro zaměstnance a klienty, jídelny pro zaměstnance, skladu spotřebního materiálu a informačních technologií, serverovny a archívu. Tyto prostory úřadu práce jsou dále rozděleny na část služební, část veřejnou a technickou. [35]

7.3.1 Technická část

Technická část obsahuje seznam, ve kterém je uveden výčet osob s oprávněním ke vstupu. Je zde umístěn též technologický deník, který obsahuje záznamy o veškerých provedených

aktivitách. Nachází se zde sklad spotřebního materiálu a informačních technologií a serverovna. Vstup do těchto místností je zabezpečen technologickým zámkem.

7.3.1.1 Serverovna

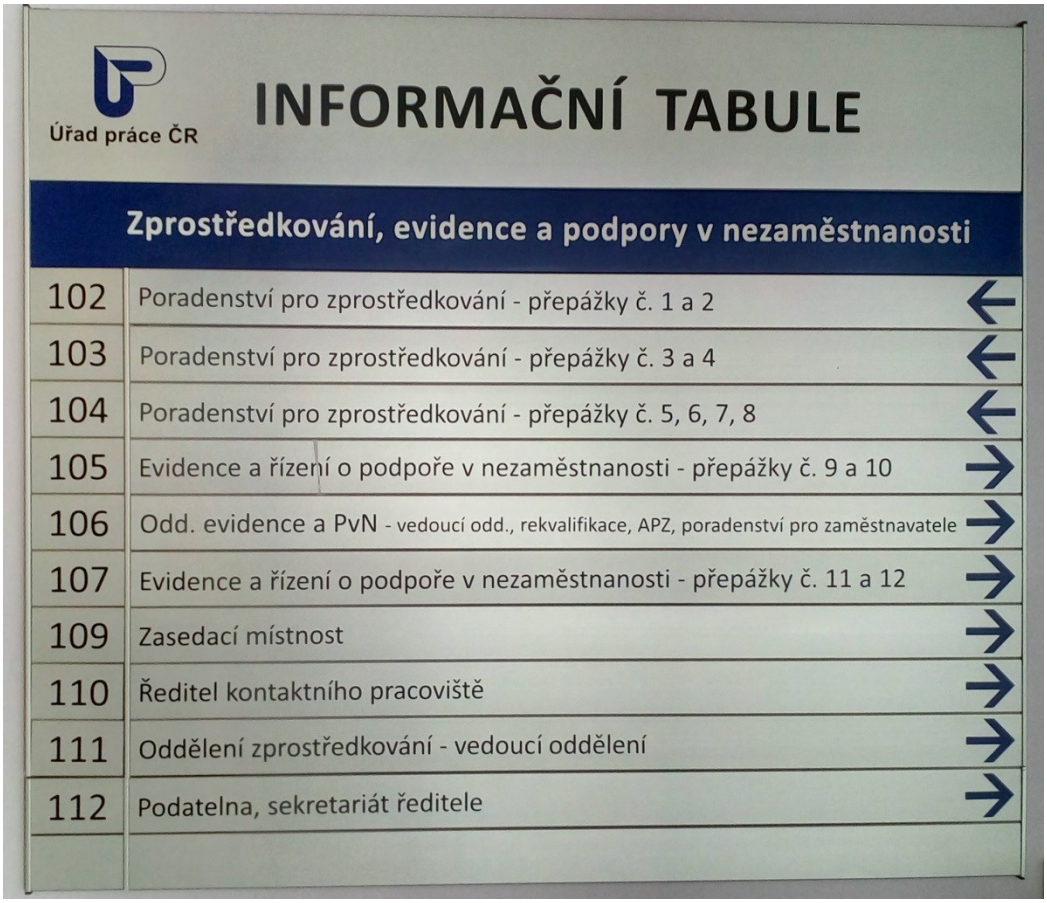
V této speciální uzamčené místnosti bez oken se nachází servery a další prvky kritické infrastruktury. Přístup do této místnosti je omezen, vztahuje se pouze na osoby s oprávněním k přístupu, tj. osoba informatika a spisové pracovnice. Tato místnost je vybavena čidly na pohyb. Aktivní síťové prvky jsou umístěny v uzamykatelné skříni v pravé části místnosti.

7.3.2 Služební část

Ve služební části se nacházejí průchozí kanceláře určené pro styk s klienty. Prostory jsou rozděleny na jednotlivé přepážky opatřené bezpečnostními prvky. Dále je zde k dispozici ke každé přepážce příruční archív tzv. „živých“ klientů, se kterými se operativně pracuje v pravidelných intervalech. K uložení „živých“ karet slouží kovové kartotéky. Mimo příruční archívy jednotlivých přepážek se v této části úřadu nachází i samostatná místnost, určená k archivaci již ukončených evidencí klientů za poslední dva roky. Jednotlivé karty jsou chronologicky seskládány dle abecedy a uloženy do speciálních kartonových krabic se štítky, které jsou dále uskladněny v regálech.

7.3.3 Veřejná část

Veřejná část prostoru úřadu práce je určená k využití samotným klientů. Jedná se o vstupní halu s čekárnou a sociálním zařízením. Jsou zde umístěny nástěnky s vyvěšenými volnými místy, které se pravidelně aktualizují jedenkrát týdně. Mimo to zde jsou na přehledných stojanech uloženy tištěné informace o možnostech využití projektů, poradenských činností a rekvalifikačních kurzů ke zvýšení uplatitelnosti klientů na trhu práce. Hlavní prioritou čekárny je však informační tabule pro klienty s popisem činností jednotlivých kanceláří. Pod tabulí je dále umístěno registrační zařízení určující pořadí a přepážku obsluhovaných klientů. V horním rohu místnosti je zavěšeno samotné vyvolávací zařízení. Klienti mohou v čekárně využít i službu informačního kiosku MPSV. Zařízení umožňuje uchazečům o zaměstnání vyhledávat pomocí integrovaného informačního portálu aktuální nabídku volných míst. [35]



Obr. 10. Informační tabule [35]

Obr. 11. Registrační zařízení [35]

Obr. 12. Informační kiosek MPSV [35]

7.4 Elektronické zabezpečení pracoviště zaměstnanosti

Zaměstnanci úřadu práce mají povolen příchod do budovy nejdříve v 6:00 hod. s nejpozdějším odchodem v 18:00 hod. Při příchodu jsou zaměstnanci povinni odkódovat chráněné prostory zadáním svého pin kódu s kombinací určité klávesové zkratky, při odchodu mají pracovníci rovněž povinnost pomocí kódovacího zařízení zajistit aktivaci ochranného prvku. Samotné operaci předchází fyzické zkontrolování všech prostor úřadu včetně sociálních zařízení s důrazem na uzavření všech okenních výplní, dále uzavření a uzamknutí všech kanceláří s kontrolou deaktivace elektronických zařízení. Jednotlivé místnosti jsou taktéž vybaveny čidly na pohyb. Identifikace a přístup uživatelů k aktivaci a deaktivaci ochranného zařízení je spravován centrálně. [35]

Obr. 13. Budova kontaktního pracoviště Kyjov [35]

8 PODSTATNÉ ASPEKTY INFORMAČNÍ A SPISOVÉ BEZPEČNOSTI ÚŘADU PRÁCE

Povinnosti k zajištění ochrany informací v oblasti informačních systémů a informačních a komunikačních technologií v podmínkách provozu informačního systému MPSV a počítačové sítě MPSV podléhá provoznímu řádu informačního systému MPSV.

8.1 Zásada mlčenlivosti

Zaměstnanec, který má přístup k osobním údajům a dále tyto chráněné informace zpracovává je povinen zachovávat mlčenlivost, pokud zvláštní zákon nestanoví jinak. Povinnost mlčenlivosti trvá i po skončení pracovního či služebního poměru. V případě, že zaměstnanec pracuje s osobními údaji nebo s chráněnými informacemi nesmí je sdělovat ani ostatním zaměstnancům úřadu a musí se vždy zachovat tak, aby nedošlo k úniku informací třetím osobám (např. volně ponechaný vytištěný dokument, odezírání z monitoru počítače apod.). Jestliže pracovník předává osobní údaje nebo chráněné informace v podobě elektronické komunikace (např. e-mailovou zprávou), je nezbytné použít šifrování k ochraně přenášené informace např. za pomoci certifikátu vydaného certifikační autoritou kartového centra MPSV. Obdobná povinnost platí i v případě vynesení informace z budovy úřadu na fyzickém nosiči (pevné disky, USB flash disky, diskety aj.). Takto užité nosiče je také nutné chránit před neoprávněným přístupem.

Zaměstnanci mají dále povinnost dodržovat pokyny provozního řádu rozlehlé datové sítě WAN MPSV, které stanovují: *„Je zakázáno využívat služeb sítě WAN pro politickou, náboženskou a rasovou agitaci nebo jiné aktivity, které jsou v rozporu se zákony České republiky. Je zakázáno neautorizované získávání, modifikace či instalace dat nebo programů. Je zakázáno neautorizované získávání nebo manipulace s jakýmikoli konfiguracemi prvků sítí nebo jiného technického vybavení“.* [36]

8.2 Spisový a skartační řád

Dalším nezbytným odpovědným krokem v oblasti bezpečnosti osobních údajů a informací je dodržování postupů stanovených ve spisovém a skartačním řádu MPSV, který vychází především ze zákona o archivnictví a spisové službě (zákon č. 499/2004 Sb.) a dalších právních norem, ke kterým řadíme zejména správní řád, zákon o ochraně osobních údajů, zákon o elektronickém podpisu aj.

Pečlivé dodržováním výše uvedeného předpisu, zejména řádnou evidencí, rychlým průběhem a neodkladným vyřízení, zajišťují všichni zaměstnanci, kteří se na práci s dokumenty podíleli. Bezpečné a přehledné ukládání neelektronických dokumentů a jejich příloh má na starosti sekretariát útvaru, který se podílel jako poslední na jejich zpracování nebo zaměstnanci tohoto útvaru, kteří dokument označili za vyřízený. Elektronický dokument je uložen do doby archivace jako příloha u příslušného čísla jednacího na počítačové síti ministerstva. Vyřízený dokument, pokud již není třeba k další průběžné práci, se předá do spisovny. Za řádný výkon spisové a skartační služby ministerstva odpovídají vedoucí útvarů v rámci své působnosti.

8.2.1 Skartační znaky a lhůta

1. Skartační znaky vyjadřují hodnotu dokumentů a nařizují, jak se s dokumenty po uplynutí skartačních lhůt bude nakládat:
    a. skartační znak „A“ (archiv) označuje archiválie (dokumenty trvalé hodnoty) a znamená, že po uplynutí skartační lhůty budou tyto dokumenty navrženy k odevzdání do archivu,
    b. skartační znak „S“ (stoupa) označuje dokumenty, které nemají trvalou hodnotu a po uplynutí skartačních lhůt se navrhnou ke zničení,
    c. skartační znak „V“ (výběr) označuje dokumenty, jejichž trvalou hodnotu nelze v okamžiku vzniku určit a znamená, že dokumenty budou po uplynutí skartačních lhůt znovu posouzeny a pak teprve označeny skartačním znakem „A“ nebo „S“,
    d. skartační znak spisu je dán nejvyšším znakem ve spisu obsažených dokumentů.
2. Skartační lhůta určuje dobu, po kterou je nutné dokumenty uchovávat ze správních a provozních důvodů. Určuje se počtem let, počítaných od 1. ledna roku následujícího po vyřízení dokumentu (u spisových celků po dni uzavření časově nejmladšího dokumentu) nebo po skončení jeho správní a provozní platnosti pro činnost úřadu. Pokud skartační lhůta není uvedena, příslušný dokument se vyřazuje v okamžiku, kdy již není potřebný pro činnost úřadu. [36]

8.3 Bezpečnostní událost

Bezpečnostní událostí rozumíme skutečnost, která se již stala a která jakýmkoliv způsobem narušila provoz systému. Mezi bezpečnostní události řadíme např. krádež nebo ztráta zařízení IS a dokumentace IS, manipulace s daty nebo softwarem, neoprávněné kopírování nosičů dat, napodobení odesílatele, neoprávněné používání systému, neoprávněné užití práv, neoprávněný vstup do chráněného prostoru, použití nelegálního software, zneužití práv správce (administrátora), ztráta důvěrnosti v důsledku možného úniku informací, ztráta integrity chráněné informace nebo osobních údajů, ztráta uložených dat atd. Všichni zaměstnanci mají poté neprodlenou ohlašovací povinnost v případě zjištění nebo podezření na výskyt bezpečností události.

8.4 Bezpečnostní politika

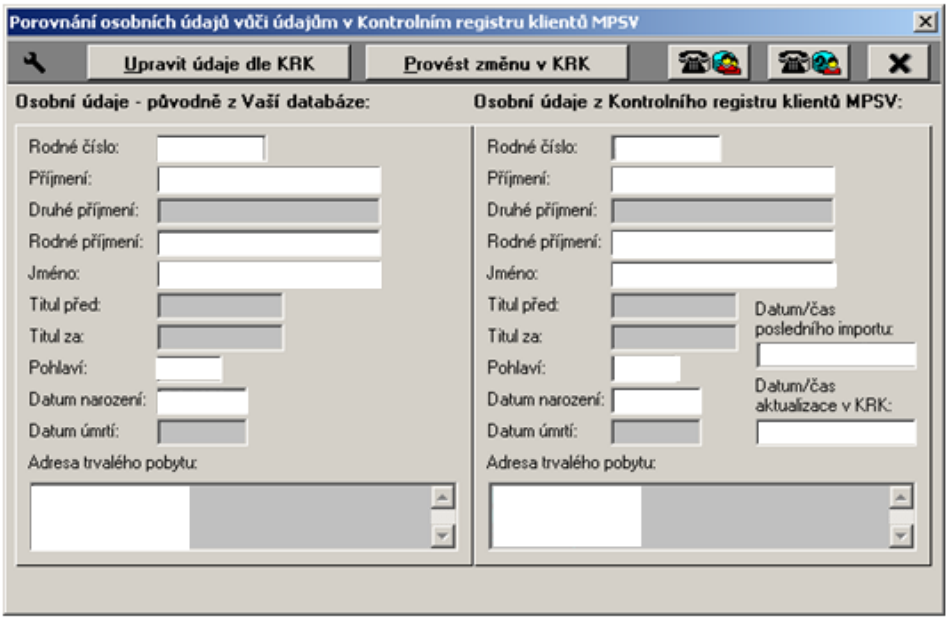
Bezpečnostní politika informačního systému MPSV zahrnuje informace obsažené v elektronické i listinné formě v prostředcích informačních a komunikačních technologií, informace v písemném i ústně sdělovaném styku. Informace MPSV je uživatel oprávněn využívat výhradně k plnění pracovních úkolů. Jakékoli jiné využití těchto informací, např. neoprávněné kopírování nebo poskytování mimo úřad, v libovolné formě, se považuje za vážné, případně hrubé porušení pracovní kázně. Vedoucí zaměstnanci všech stupňů odpovídají za realizaci Bezpečnostní politiky MPSV v rámci jejich působnosti. Jsou povinni prosazovat Bezpečnostní politiku informací do praxe, vést své podřízené k dodržování této Bezpečnostní politiky a plnění stanovených zásad bezpečnosti informací v denní praxi. [36]

9 POSTUP PRACOVNÍHO PROCESU V OBLASTI ZPROSTŘEDKOVÁNÍ ZAMĚSTNÁNÍ A PODPORY V NEZAMĚSTNANOSTI

Klient je povinen se osobně dostavit na kontaktní pracoviště úřadu práce, do jehož krajského územního obvodu dle svého trvalého bydliště spadá. Po předložení platného občanského průkazu zadá zaměstnanec úřadu práce do informačního systému OKpráce rodné číslo klienta a ten je poté vyhledán v databázi zmíněného programu. Pokud již občan byl v minulosti evidován na navštíveném KoPu, je jeho osoba v databázi dohledatelná a můžeme tak pokračovat v založení evidence nové.

Pokud se nejedná o opakovanou evidenci klienta, musí být jeho osobní údaje načteny z kontrolního registru MPSV označovaného zkratkou KRK. Pokud KRK osobní údaje neobsahuje, je nutné tyto údaje do IS OKpráce ručně doplnit a poté načíst do kontrolního registru. Pouze tímto způsobem může být uchazeči o zaměstnání přidělen identifikátor IK MPSV, v programu OKpráce zobrazováno jako ID číslo.

Dále je nezbytné sledovat aktuálnost údajů v KRK. Při ukládání dat informační systém OKpráce automaticky oznamuje nekonzistenci osobních údajů mezi KRK a IS OKpráce. V takovém případě musí být vyhodnoceno, zda údaje vedené v KRK přijmout či nahradit aktuálními údaji vedenými v IS OKpráce. Tyto situace nastávají zejména při opakovaných evidencích uchazečů o zaměstnání.



Obr. 14. Porovnání osobních údajů klientů v IS [36]

Může se též stát, že občan byl v minulosti evidován na jiném pracovišti úřadu práce. V takovémto případě je nutné nejprve sehrát data klienta z předchozí evidence na domovské pracoviště, aby nedošlo ke vzniku tzv. duplicitní evidence. [35]

9.1 Podání žádosti o zprostředkování zaměstnání

Prvním krokem v oblasti zprostředkování je vlastnoruční vypsání Žádosti o zprostředkování zaměstnání klientem na úřadu práce. Veškeré údaje poskytnuté občanem přeneseme z písemné podoby do elektronické. Při zakládání nové evidence občana vždy dbáme na vyplnění všech důležitých údajů o klientovi. Jedná se tedy především o aktuální místo trvalého bydliště, kontaktní údaje, doručovací adresu, zdravotní stav, nejvyšší dosažené vzdělání se samotným oborem vzdělání, dovednosti a praxe uchazeče, požadavky na zaměstnání a v neposlední řadě pak údaje o poslední ukončené činnosti (např. zaměstnání). Všechny doložené doklady (např. zápočtový list, doklad o ukončení pracovního poměru, lékařské potvrzení, potvrzení o době studia, doklad o nejvyšším dosaženém vzdělání aj.) opatříme čárovým kódem, datem doložení, razítkem ověření a razítkem délky skartace. Po zařazení klienta do databáze uchazečů o zaměstnání vyhotovíme kontaktní list obsahující zápis uskutečněného jednání, ve kterém je uvedeno, co uchazeč o zaměstnání (UoZ) doložil na úřad práce a co naopak obdržel.

Na základě vyplněných údajů úřad práce dále spolupracuje s uchazečem o zaměstnání na pravidelných schůzkách v určených dnech a čase za účelem naleznutí vhodného zaměstnání, případně pomoci klientovi doplnit jeho stávající kvalifikaci vhodnou rekvalifikací nebo zařazením do poradenského programu či jiného projektu financovaného z prostředků evropského sociálního fondu.

9.2 Podání žádosti o podporu v nezaměstnanosti

V případě podání žádosti o podporu v nezaměstnanosti postupujeme obdobným způsobem, jako při podání žádosti o zprostředkování zaměstnání. Při podání žádosti o podporu v nezaměstnanosti (PvN) zkoumáme posledních 24 měsíců od data podání žádosti o PvN. Pokud uchazeč o zaměstnání v tomto posuzovaném období doloží 12 měsíců, ve kterých byl důchodově pojištěn ať už ze statutu zaměstnance nebo osoby samostatně výdělečné činné, bude mu přiznána podpora v nezaměstnanosti. Tyto skutečnosti osvědčí např. evidenční listem důchodového pojištění, doklady z Okresní správy sociálního zabezpečení, dokladem E 301 a U 1 v případě doby zaměstnání v zahraničí a náhradními doklady důchodového

pojištění (v případě osobní péče o dítě do 4 let, péče o osobu závislou, doba pobírání invalidního důchodu třetího stupně, trvání dočasné pracovní neschopnosti aj.).

Pokud spočívala poslední činnost klienta v zaměstnání, dokládá také potvrzení o výši jeho průměrného popřípadě pravděpodobného čistého měsíčního výdělku, ze kterého bude PvN vypočítána a způsob ukončení pracovního poměru. Klient si také sám stanoví způsob výplaty dávky. PvN je možné zaslat poštovní poukázkou na doručovací adresu občana nebo na bankovní účet. Při volbě „poštovná poukázka“ je nutné vyplnit souhlas s předáním rodného čísla České poště, který uchazeč o zaměstnání uděluje v žádosti o zprostředkování zaměstnání.

Pokud klient nesplnil výše požadované podmínky, obdrží rozhodnutí o nepřiznání podpory v nezaměstnanosti. Jestliže uchazeč nemůže do 30 dnů ode dne podání žádosti o PvN z prokazatelných důvodů doložit dobu důchodového pojištění, vystaví úřad práce usnesení o přerušení řízení ve věci žádosti o podporu v nezaměstnanosti na žádost žadatele. V tomto usnesení bude uvedena lhůta, do které je nezbytné požadované doklady doložit, po vypršení této lhůty bude ve věci podpory v nezaměstnanosti rozhodnuto. Tato problematika včetně oblasti zprostředkování zaměstnání je právně ukotvena zákonem č. 435/2004 Sb. o zaměstnanosti, ve znění pozdějších předpisů.

9.3 Ukončení evidence úřadu práce

V případě, že úřad práce zprostředkuje klientovi vhodné zaměstnání za pomocí doporučenky do zaměstnání nebo si zaměstnání uchazeč najde sám, dochází k ukončení evidence oznámením o nástupu do zaměstnání a doložením příslušného dokladu o nástupu. Další možností je například zahájení samostatně výdělečné činnosti, která též brání v pokračování evidence. Uchazeči se mohou vyřadit i na vlastní žádost bez udání důvodu. Další překážkou může být také zdravotní stav, který klientovi nedovoluje se dále ucházet o zaměstnání (přiznání invalidity III. stupně). V poslední řadě dochází k úmrtí klienta, kdy je evidence na základně úmrtního listu ukončena dnem úmrtí.

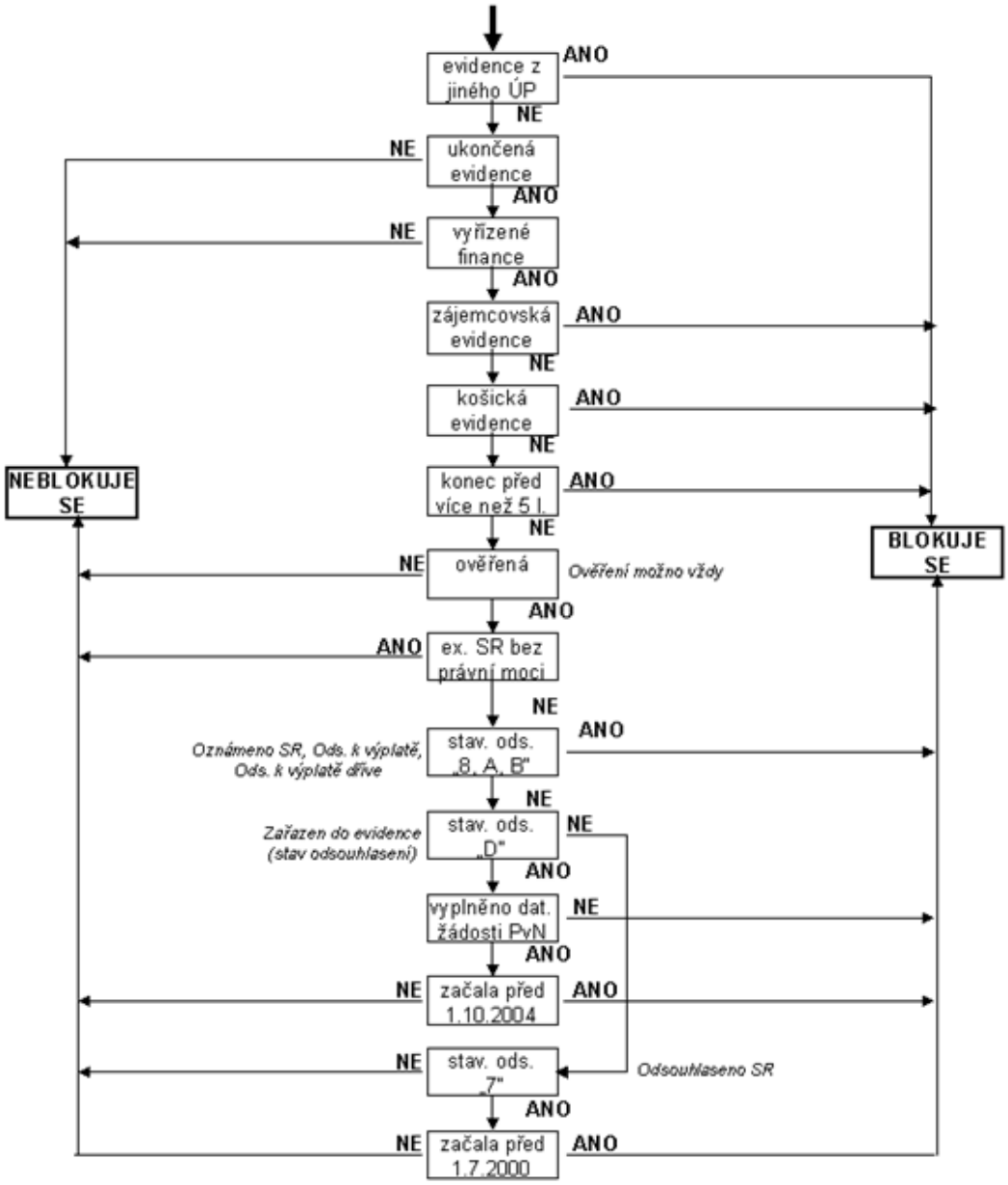
9.3.1 Sankční vyřazení uchazeče o zaměstnání

Pokud nastane některá skutečnost bránící zařazení a vedení v evidenci uchazečů o zaměstnání a uchazeč nesplní oznamovací povinnost nejpozději do 8 kalendářních dnů a to bez vážných důvodů dochází poté k vyřazení klienta z evidence UoZ. Tato skutečnost může nastat například, pokud klient neoznámí skutečnosti, které mají vliv na zařazení a vede-

ní v evidenci UoZ - např. nenahlásí nástup do zaměstnání, neoznámí výkon nekolidujícího zaměstnání, neoznámí osobně nebo písemně důvody, pro které se nemohl dostavit na kontaktní pracoviště, dále neoznámí důvody, pro které není dočasně schopen plnit povinnosti UoZ aj. V dalších případech, které mohou nastat, a je za ně uchazeč postižen vyřazením z evidence, je např. odmítnutí nástupu do vhodného zaměstnání nebo na dohodnutou rekvalifikaci, dále neposkytne nebo maří součinnost s úřadem práce. V těchto případech je uchazeč postižen sankcí za porušení svých povinností vůči úřadu práce. Podstatou sankce je nemožnost uchazeče opětovně se vrátit do evidence úřadu práce po dobu několika měsíců (3 nebo 6).

Jakmile je evidence klienta ukončena, dochází k uložení jeho spisové dokumentace do archívu kontaktního pracoviště úřadu práce, kde je spis uchován po dobu dvou let. Po uplynutí doby je dokumentace převezena do centrálního skladu.

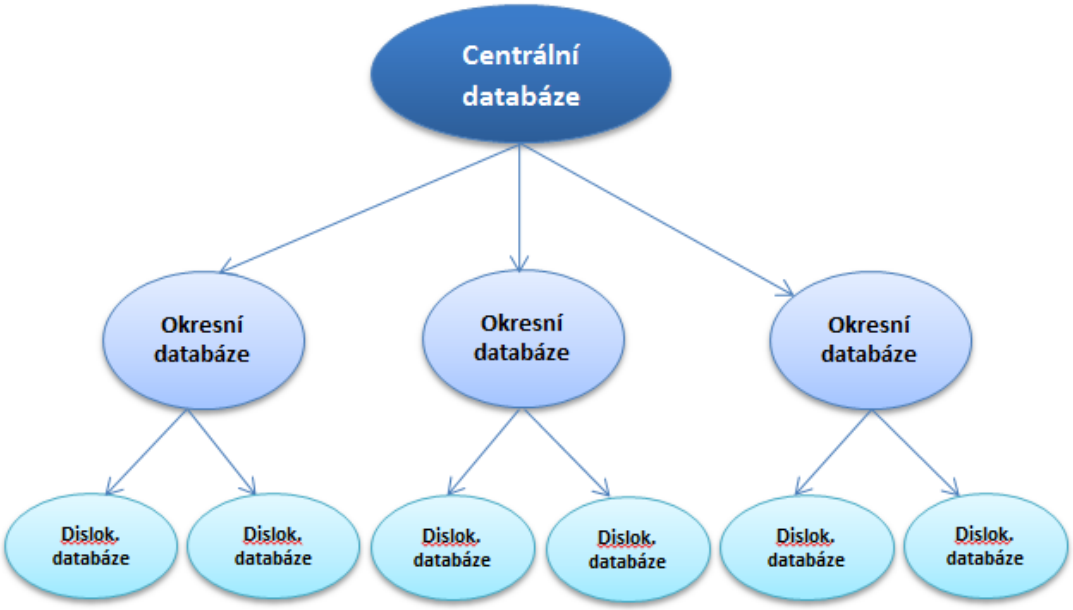
Po zkontrolování správnosti všech náležitostí elektronického i fyzického spisu je již vyřazený klient v databázi zablokován a není možné s ním nadále pracovat. Pouze oprávněná osoba má možnost provést odblokaci klienta pro dobu nezbytně nutnou k provedení potřebné operace, ihned po uložení změn dochází opět k zablokování. Takovýmto způsobem je možné přesně identifikovat veškeré změny prováděné s údaji klienta v informačním systému. [35]



Obr. 15. Vyhodonocování funkce blokování pro evidenci [36]

10 STRUKTURA INFORMAČNÍHO SYSTÉMU ÚŘADU PRÁCE

Úřad práce ČR provozuje na celém svém území síť poboček úřadu práce, které jsou rozděleny do tří úrovní. Nejvyšší úrovní je úroveň centrum. V tomto místě jsou uloženy centrální databáze. Z bezpečnostního důvodu je datové centrum každé aplikace zdvojeno. Druhou úrovní jsou úřady okresní a třetí úrovní jsou úřady dislokované podřízené okresním úřadům. Toto uspořádání odpovídá z historických důvodů územně správnímu členění České republiky.



Obr. 16. Schéma databází úřadu práce [35]

Z důvodu rozsáhlosti agendy ÚP je provozováno několik informačních systémů, které pokrývají oba typy struktur rozsáhlých databází, které nás zajímají. [36]

10.1 Informační systém státní sociální podpory

Státní sociální podpora (SSP) provozuje dva druhy informačních systémů, které pokrývají potřeby práce s klienty. Tyto IS jsou postaveny na modelu centrální databáze a jednotlivých klientů. Všichni klienti jsou rovnocenní a rozsah jejich možností je stejný. Centrální databáze je typu SQL. Z důvodu bezpečnosti a rozložení zátěže existuje ve dvou exemplářích. Jedna z těchto centrálních databází je umístěna v záložním datovém centru. Klientské programy těchto IS jsou nazývány lehkými. Jsou vytvořeny ve vyšším programovacím jazyce - JAVA nebo SILVERLIGHT. Aplikace při spuštění zkontroluje svou aktuálnost

a případně se nahraje z centra v aktuální verzi. Její činnost probíhá v okně prohlížeče. Tento druh databáze IS provozovaný na SSP není předmětem dalšího popisu.

10.2 Informační systém služby zaměstnanosti

IS služby zaměstnanosti je tvořen lokálními databázemi, které jsou hierarchicky postaveny jako distribuovaná hvězda. Topologie je podobná jako u počítačových sítí typu distribuovaná hvězda. Centrální databáze je nejvýše umístěná v hierarchii a kompletní obsah IS je uložen v ní a v její duplicitní kopii. Na ní napojené databáze okresních pracovišť obsahují pouze územně relevantní data podle trvalého (přechodného) bydliště klientů. Na úrovni okresu je k této databázi připojen systém podřízených dislokovaných pracovišť. Tyto databáze nejnižší úrovně rozčleňují okres (pokryté území) na dále již nedělitelné celky. Jsou podmnožinou okresní databáze.

Stěhování uchazečů je provedeno tak, že při tomto úkonu si uchazeč nese s sebou celou historii svých evidencí. Při dalších případných stěhováních se postup opakuje. Historická data uchazečů zůstávají zachována v databázi a jsou pouze uzamknuta.

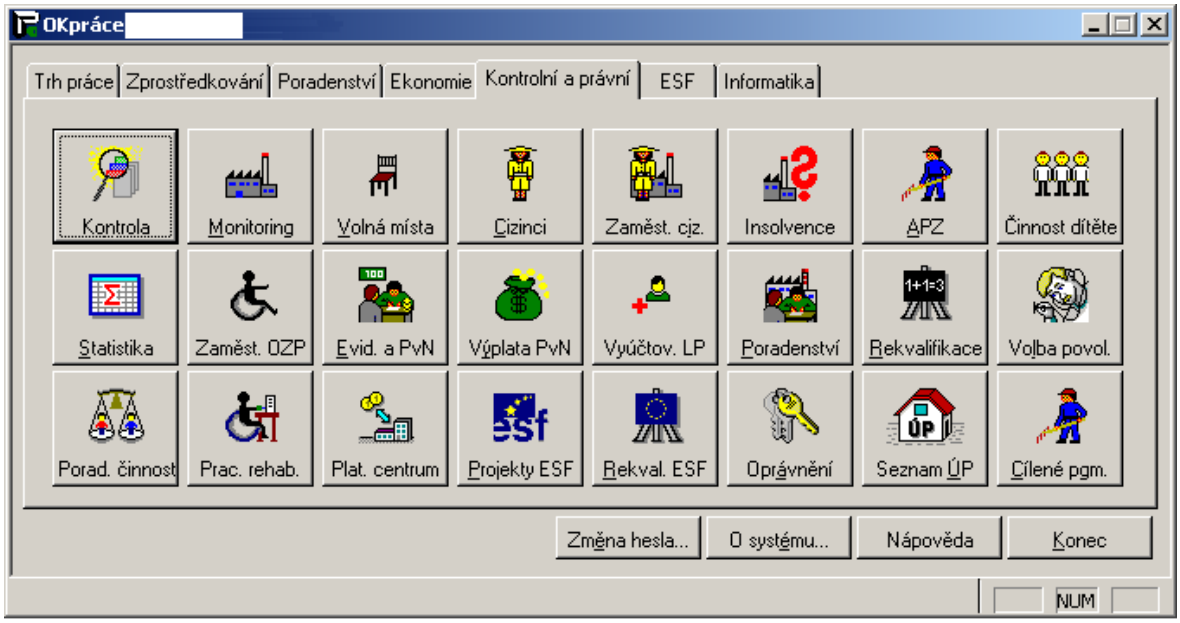
Synchronizace dat celé hierarchie databáze probíhá pomocí generování datových balíků. Synchronizace je obousměrná s 24 hodinovým cyklem. Datové balíky obsahuj informace zahrnující přesuny klientů mezi okresy, rozšíření registru objektů v obcích, které tito klienti obývají. Dále jsou zde soustředěny informace o dalších aktivitách, které jsou celostátně koordinovány. Týká se to zejména poskytování a využití volných míst, rekvalifikací klientů a informacích o školně vzdělávacím systému.

Klient tohoto IS není jako v předchozím systému lehký, ale plnohodnotně napsaný jako aplikace pro PC s operačním systémem Windows. Klient je distribuován na jednotlivé stanice vždy při instalaci nové verze databáze. Toto probíhá v pravidelném cyklu, který je doplňován o aktuální opravy chyb. Proces je kontrolován informatikem na úrovni přípravy aktualizací a nasazení. Aktualizace programového vybavení stanic potom probíhá synchronizací podle vzoru.

Jednotlivý klient na pracovní stanici je dále členěn do pracovních modulů. Pracovník může mít současně otevřeno několik modulů. Tedy může například provádět zprostředkování zaměstnání a k tomu vyhledávat pro daného klienta možnou rekvalifikaci. Aby toto mohlo korektně probíhat, činnosti klienta jsou rozděleny na povolné - souběžné a výlučné neboli kolizní. Kolizní činnosti jsou ty, u kterých by mohlo dojít k zneužití informací nebo

při finančních operacích prováděných informačním systémem. Tedy například pracovníci provádějící výplaty nemohou ovlivnit jejich výši, případně jestli daný klient má nebo nemá nárok. Veškeré transakce v tomto IS jsou doplněni jménem pracovníka, který je provedl. V rámci provozu databáze jsou údaje synchronizovány již uvedeným postupem do centrální databáze. Archivace dat probíhá pro nutnou dobu danou zákonem. [36]

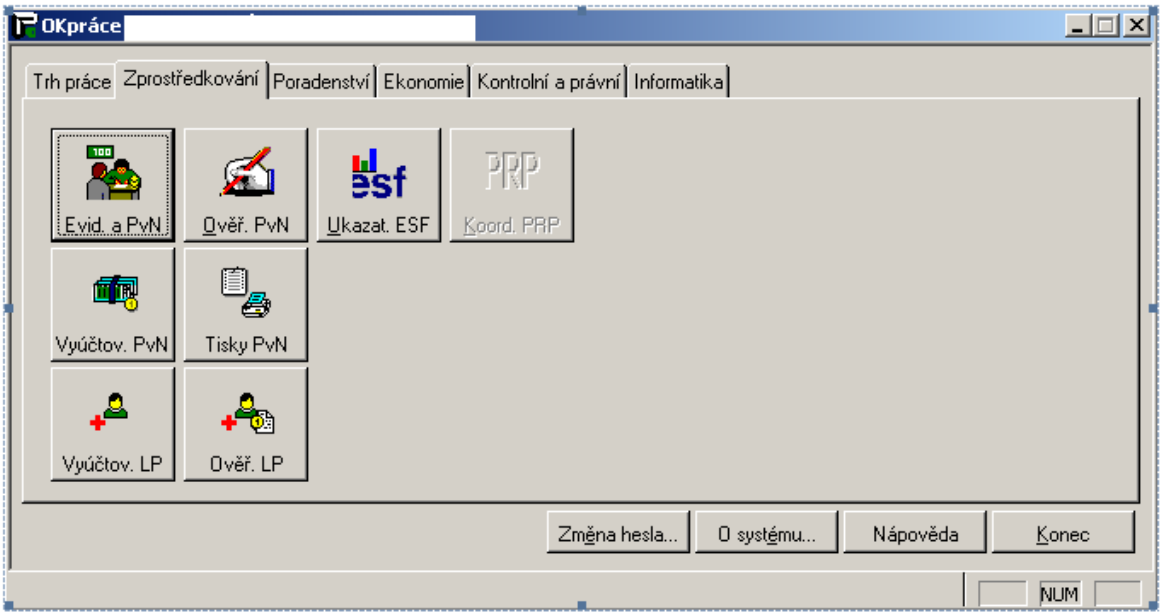
Na následujících obrázcích je uvedeno pracovní pozadí informačního systému OKpráce, sloužícího pro službu zaměstnanosti. Uvádí vyobrazení jednotlivých odborů, do kterých je příslušný uživatel zařazen.



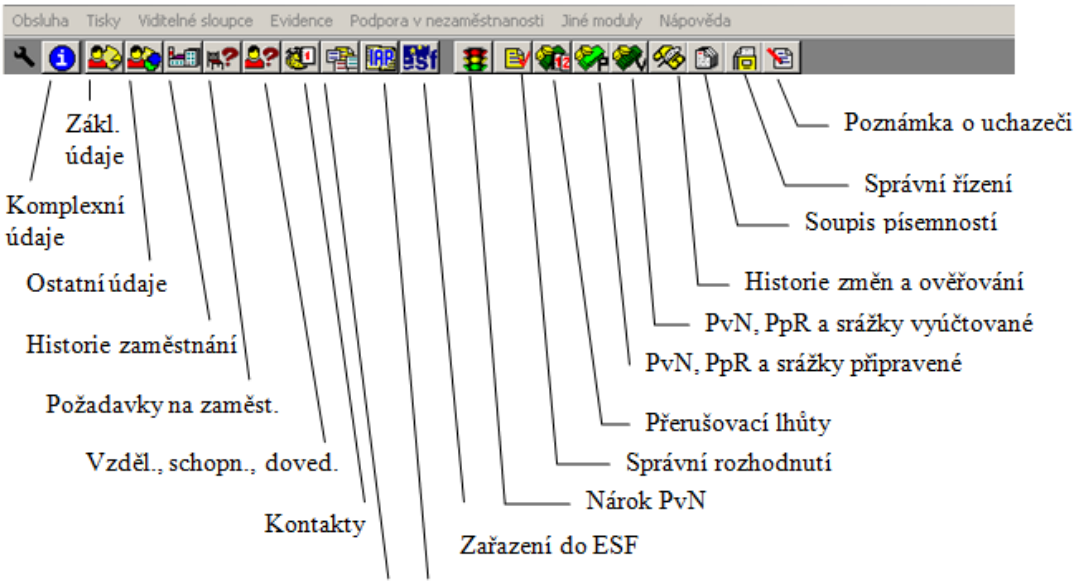
Obr. 17. Záložky IS jednotlivých odborů ÚP [36]

Každá z vyobrazených záložek obsahuje tlačítka pro spuštění modulů určených pro práci na příslušném odboru. Tlačítka modulů, která nejsou přístupná, značí fakt, že uživateli nebyla k těmto modulům přidělena přístupová práva.

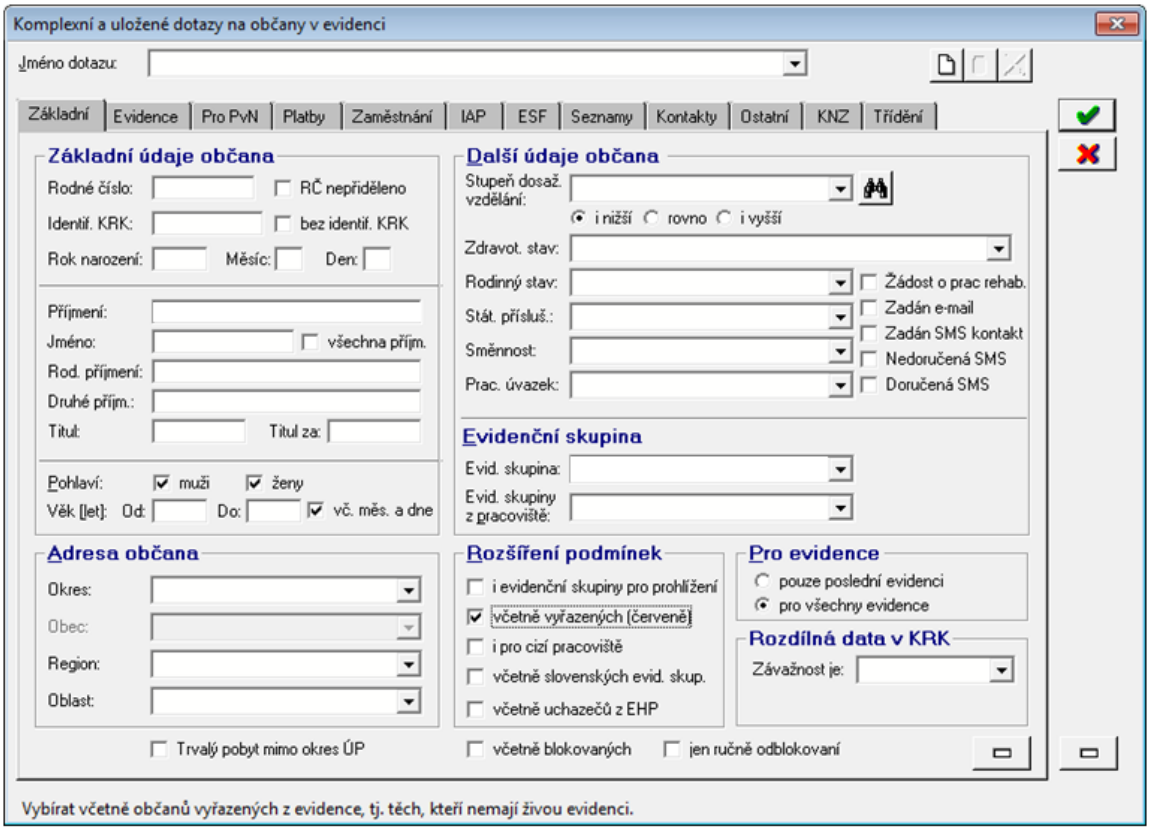
Další obrázky znázorňují popis základních dostupných ikon IS a možnosti vyhledávání osobních údajů občanů v jednotlivých oknech IS OKpráce v sekci Zprostředkování - Evid. a PvN dle požadovaných kritérií typu základní údaje občana (rodné číslo, příjmení, bydliště, zdravotní stav aj.), délka evidence a nárok na podporu v nezaměstnanosti.



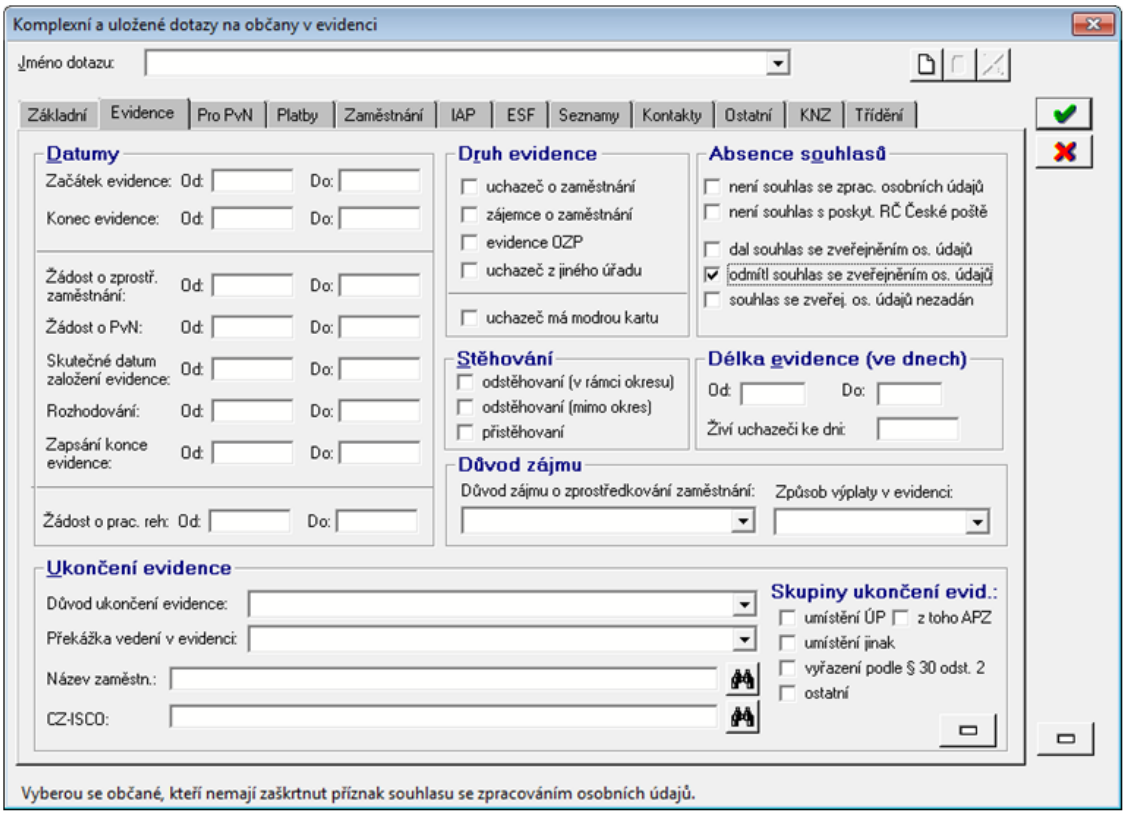
Obr. 18. Záložka odboru zprostředkování zaměstnání ÚP [36]



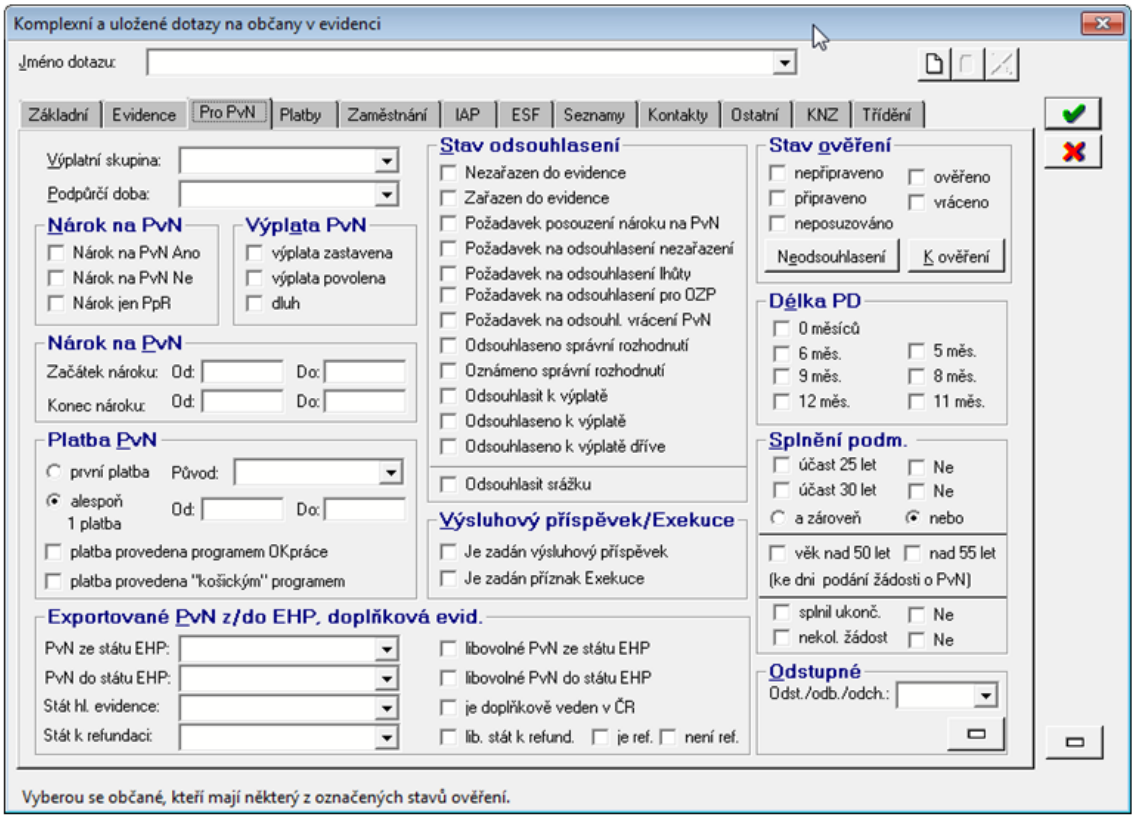
Obr. 19. Základní ikony IS OKpráce [36]



Obr. 20. Výběrové okno IS dle základních údajů klienta ÚP [36]



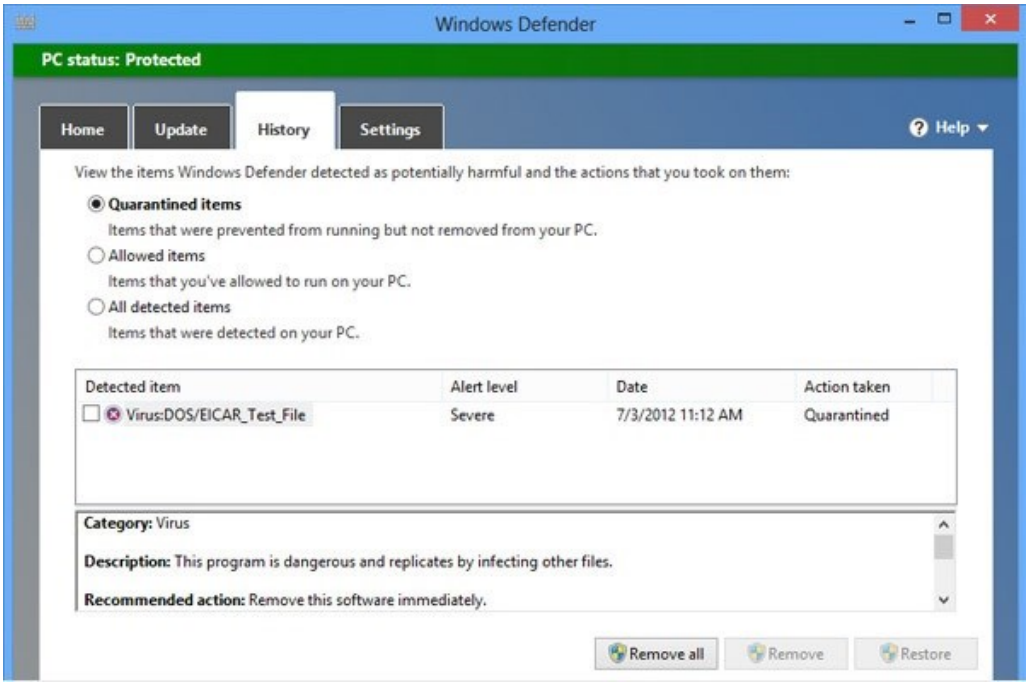
Obr. 21. Výběrového okno IS dle podmínek evidence [36]



Obr. 22. Výběrové okno IS dle posouzení nároku na PvN [36]

11 ANTIVIROVÁ OCHRANA A OCHRANA ELEKTRONICKÉ POŠTY

Rozsáhlá datová síť MPSV je oddělena od sítí veřejných. A to jak od ostatních ministerstev, tak státních orgánu ČR a též od internetu. Propojení této sítě je nutné zajistit tak, aby nebylo možné proniknout dovnitř, případně zcela obejít řízený datový provoz. Nejčastějším případem napadení internetové brány je útok zvaný DDOS. Jeho důsledkem dojde k přetížení hraničních serverů a tyto propustí útočníka do vnitřní sítě. Aby k tomu nedošlo, jsou tyto chráněny specializovaným programovým vybavením. Každý přenos dat požadovaný ze sítě směrem ven má svého žadatele, což je obvykle uživatel, aplikace, systémová služba apod. Pokud je zjištěn neautorizovaný požadavek pro přístup z vnitřní sítě přes tuto bránu je uložen do bezpečnostních záznamů. Další součástí zabezpečení je analytický program, který sleduje neoprávněné pokusy o přístup a dělí je do kategorií podle nebezpečnosti. Bezpečnostní odbor v zastoupení fyzického zaměstnance analyzuje záznamy a přijímání opatření. [36]



Obr. 23. Antivirový klient - Windows defender [37]

11.1 Systém intranetu

Vstupně výstupní systém intranetu filtruje požadavky na přístup k webovým službám a webovým stránkám v součinnosti s nastaveným seznamem. Tento měsíčně aktualizovaný soubor obsahuje webové adresy stránek, které nelze navštěvovat. Důvodem může být jak

škodlivý obsah, tak to, že obsah nesouvisí s předmětem služební činnosti. Kategorie jsou dále členěny podle stupně oprávnění, kdy bez omezení je možný přístup např. informatikům a některým manažerům. Z datových služeb „služby na vyžádání“ jakou jsou youtube, spotifi nebo jiné, které poskytují video a audio obsah jsou téměř zcela omezeny. Důvodem je vysoké zatížení přenosových cest. Výjimku z tohoto mají pouze vzdělávací odbory ÚP (IPS poradci pro volbu povolání).

Antivirové zabezpečení intranetu je zajištěno programem na stanicích a serverech dodávaných výrobcem operačního systému. Některá zařízení jsou zabezpečena programovými prostředky třetích stran (MCAFFEE, Symantec apod.). MPSV jako subjekt velkého rozsahu působí na uzavřenou smlouvu o dodávkách antivirových vzorků a definic s vysokou prioritou. To znamená, že dostává své bezpečnostní aktualizace několikrát častěji než běžný uživatel. I z toho důvodu je celý antivirový systém centrálně spravovaný z Centra. Vztah jednotlivé definice si jednotlivé stanice nesestavují sami, ale jsou jim zasílány technologií „push“. Všechny stanice proto obsahují známou verzi antivirových definic a lze tedy v každém okamžiku říci, jestli jsou odolné vůči určitému druhu napadení.

11.2 Aktualizace antivirového programu

Aktualizace antivirového programu je prováděna centrální instalací. V případě vydání nové verze antivirového programu dojde k záměně se starou verzí v řádu několika málo hodin. V případě delšího nepoužití pracovní stanice je instalace provedena ihned po zapnutí stanice. Kontrola stanic v reálném čase na přítomnost virů a úplná kontrola jejich pevných disků je taktéž spravována centrálně řídicím programem v centru. Dodavatelem je stejně jako v případě IS firma Microsoft.

11.3 Elektronická pošta

MPSV spravuje několik domén elektronické pošty. V nedávné době došlo k nahrazení domén obsahující jméno okresu centrální doménou @uradprace.cz. Část před doménovým jménem je tvořena jménem příjmením a případně pořadovým číslem zaměstnance - např. veronika.zamecnikova@uradprace.cz. Bylo tedy upuštěno od lokalizace držitele pomocí domény e-mailu a tyto nejsou dále územně členěné. Jako klient elektronické pošty se používá Microsoft Outlook s několika rozšířeními. Poštovní klient je navázán na identitu uživatele, při jeho prvním přihlášení založí elektronickou schránku a nastaví komunikaci.

11.3.1 Ochrana elektronické pošty

Takto rozsáhlou síť je nutné chránit proti spamu a šíření nebezpečných obsahů e-mailů. Nevyžádaná pošta je nalezená a odstraněná na úrovni poštovních serverů v Centru. Jako nástroj se používá komerčně dostupný produkt třetí strany. Pro třídění využívá jak seznam nežádoucích odesílatelů a domén, tak tzv. bayesovský filtr. Tento filtr tvoří samo se učící entitu. Uživatelé zpětnou vazbou potvrzují, zda daný e-mail byl nebo nebyl spamem. Jejich rozhodnutí se statisticky vyhodnotí. Tímto vznikne rozhodnutí o tom, jak vypadá aktuální typický spam. Získaný vzorec je poté aplikován na podobné podezřelé objekty.

Častou přílohou elektronické pošty jsou dokumenty, které obsahují škodlivý obsah. Mohou to být přímo spustitelné programy (v jazyce JAVA), odkazy na nebezpečné internetové stránky nebo makra vložená například do souborů Word. Ochranný software na poštovním serveru tyto přílohy najde, odstraní a doplní text o jejich odstranění. Pokud je přílohou komprimovaný datový archiv, je tento rozbalen a zkontrolován. Pokud je chráněn heslem je odstraněn stejně jako škodlivé přílohy. [36]

Největším nebezpečím v elektronické komunikaci jsou přístupy na webová rozhraní poštovních klientů v internetu - např. seznam.cz, google.com, email.cz aj. Tyto servery nejsou zakázány. Jejich obsah však projde standartní cestou jako jakékoli jiné data. Proto je kontrolován co do škodlivosti standartními antivirovými prostředky. Neuplatní se tedy specializovaný software pro kontrolu e-mailu jako v případě elektronické pošty.

Prostředky ochrany proti zneužití a napadení jsou aplikovány na vlastní datový přenos mezi pobočkami, respektive v celé síti. Prostý, nešifrovaný provoz probíhá pouze mezi stanicí a prvním směrovacím prvkem sítě. Na tomto komunikačním prvku jsou přenášená data zašifrována. Dále jsou opatřena časovou značkou a adresou původu. Časová značka umožní zjistit, jestli nebyl datový balíček dešifrován hrubou silou (což nějakou dobu trvá). Označení odesílatele slouží při zpětném návratu datového balíčku, aby znemožnil identifikaci konkrétního počítače komunikujícího po síti. Někdy se tato technologie nazývá „maškaráda“. Samotné šifrování provádí komunikační prvek technologií, která není veřejně známa. Spoléhá se při tom na to, že všechny důležité místa jsou nakonfigurována na zařízení stejné firmy (Cisco apod.). [36]

12 ZÁLOHOVÁNÍ DAT

12.1 Zálohování serverů

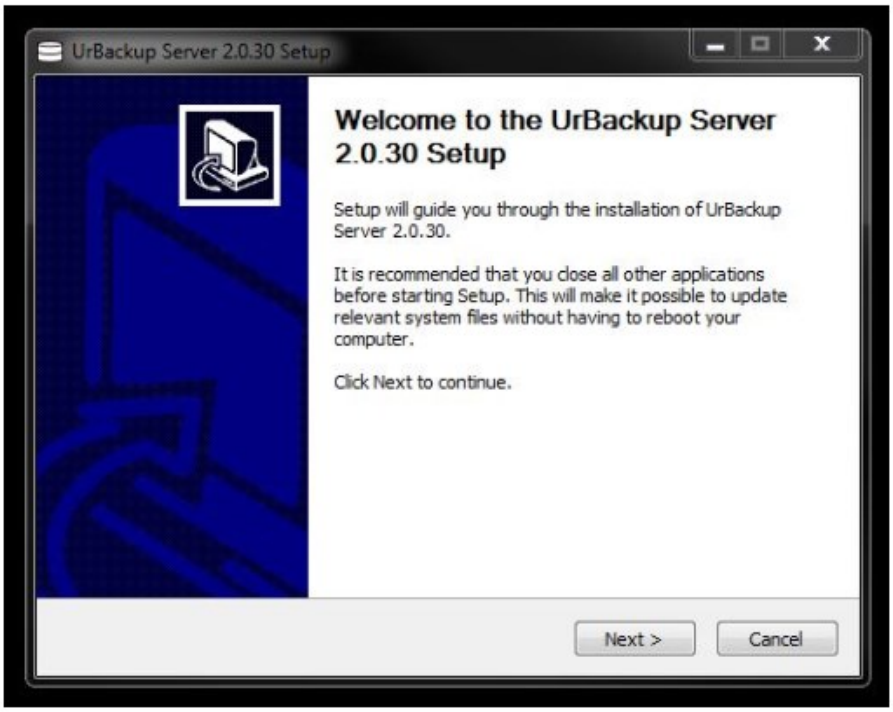
Servery provozované na úřadu práce jsou produkty firmy Microsoft ve verzích 2003 - 2016. V převážné míře se jedná o servery fyzické. V posledním roce bylo přistoupeno k nasazení serverů virtuálních.

12.1.1 Zálohování fyzických serverů

Fyzické servery od verze 2003 výše jsou zálohovány pomocí tzv. „zálohy za běhu“. To znamená, že po dobu zálohy je zastavena většina systémových služeb. Důsledkem je, že na discích dochází k minimálním změnám v datech. Zálohovací program postupně nakopíruje na vzdálený disk všechny sektory, které najde na serveru, jenž zálohuje. Tento vzdálený disk je umístěný v téže počítačové síti obvykle ve stejné lokalitě. Uvedený proces je prováděný pro celý server vyjma oddíly obsahující data uživatelů případně databáze. Pro daný účel lze použít v nejjednodušším případě triviální utilitu HDD2VHD. Tato provede výše uvedené zálohování disku. V kombinaci s několika dávkovými soubory jsou takto vytvořené obrazy ukládány a spravovány. Používá se zálohování v cyklu jednoho měsíce a potom také před závažnými změnami softwarového vybavení.

12.1.2 Zálohování virtuálních serverů

Virtuální servery jsou provozovány na tzv. hostiteli. Při pohledu na disky hostitele vidíme každý jednotlivý server jako adresář obsahující jeden nebo několik velkých souborů. Tyto soubory obsahují v podstatě celý server včetně všech dat uživatelů případně včetně všech databází. Microsoft dodává komplexní řešení provozu zálohování a obnovy těchto virtuálních serverů. Pro ukládání dat záloh jsou v síti určeny servery, které přímo mají úlohu backup serveru. Každý backup server (může být i více) obsluhuje nejméně jeden virtuální server. Tento je pro něj vlastně klientem, jehož data chrání.



Obr. 24. Instalace serverové části UrBackup [38]

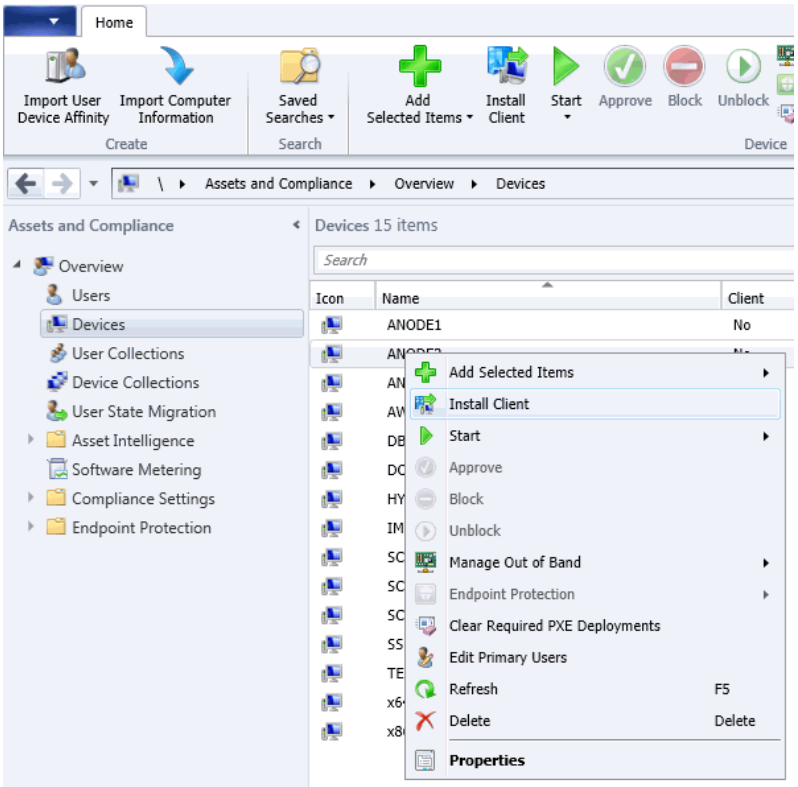
Celý proces zálohování je možné provádět za chodu bez omezení funkčnosti jakékoli služby, která na virtuálním serveru běží. Proces, kterým se to provádí, nazýváme „snap shot“. Během něj zálohovací server postupně zkopíruje všechny sektory zálohovaného serveru. Pokud se nějaké během procesu zálohování změnily, provede jejich uložení znovu. Aby se zvýšila úspěšnost této metody zálohovací server je schopen zálohovanému klientovi na nutnou dobu pozastavit činnost. Jedná se o proces zvaný freeze neboli zamrazení. Uživatelé serverů tento proces nijak neomezí, protože je velmi krátký, řádově několik sekund. Zálohovací server provozuje svoji činnost pomocí tzv. úplných a inkrementálních obrazů virtuálních serverů. Úplný obraz je poměrně veliký. Inkrementální obraz postihuje pouze změny před současným a předchozím stavem a jeho velikost bývá řádově menší. I při tomto zálohování správce zálohovacího serveru nastavuje cyklus záloh. V našem případě jde o cyklus týdenní. Plná záloha se provádí ve volný pracovní den, inkrementální záloha pak postihuje změny vzniklé v jednotlivých pracovních dnech. Cyklus týdenních záloh se opakuje s měsíčním cyklem, kdy se zachovává každá čtvrtá záloha. Tato čtyřtýdenní záloha není nikdy starší než půl roku.

Zálohování databáze běžící ve virtuálním serveru je možné tenkrát, pokud jsou soubory databáze postiženy změnami pouze v malém rozsahu. Při běžném provozu relační databáze

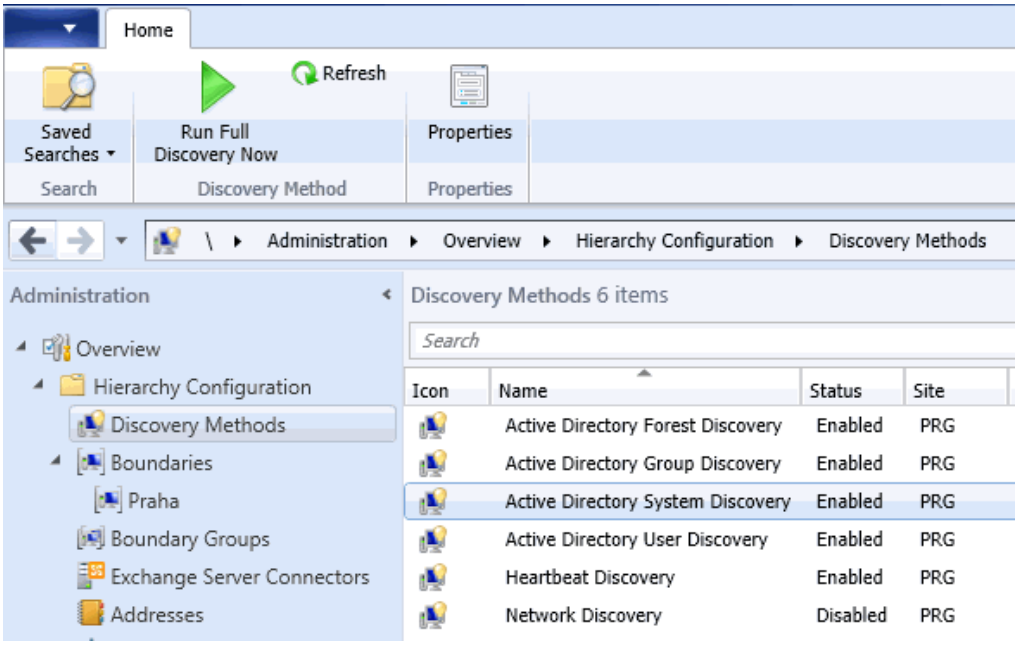
typu SQL však tuto podmínku splňuje s výhradami. Dá se říci, že bychom při každé inkrementální záloze virtuálního serveru tuto zálohovaly z více jak jedné třetiny. [36]

12.2 Zálohování stanic

Pracovní stanice uživatelů jsou na úřadu práce klasifikovány do několika málo tipů. Při nákupech se dbá na to, aby HW platforma nebyla roztříštěna a byla co nejvíce jednotná. Proto je možné pomocí standardizovaných postupů stanici instalovat z tzv. obrazu stanice. Tyto obrazy se pravidelně aktualizují servisními balíčky. V případě zavedení nového programového vybavení je toto instalováno i do instalačního obrazu stanice. Z tohoto důvodu se zálohování samotných stanic neprovádí. Jejich obnova z obrazu je časově méně náročná. Protože je obraz anonymizovaný (musí se pro obnovení stanice provést dokončení konfigurace). Pro tuto činnost používáme Microsoft SCCM. Takto je nazýváno komplexní prostředí pro správu a nastavování stanic. Po přidání stanice do domény jsou na ni aplikována pravidla a nastavení, které určil správce domény. Tyto parametry se modifikují dle toho, z jakého fyzického umístění žádá stanice o zařazení do počítačové sítě. [36]



Obr. 25. Instalace klienta SSCM na stanici [39]



Obr. 26. Nastavení a konfigurace vyhledáváni stanic pro instalaci klienta SSCM [39]

12.3 Zálohování dat uživatelů

Data uživatelů na stanici jsou duplikována při přihlašovacím procesu ze serveru procesem tzv. cestovního profilu. Na jakékoli stanici se uživatel přihlásí, tam jsou jeho data ze serveru zkopírována. Při odhlašování uživatele jsou veškerá změněná data zkopírována zpět na server. Tím je zjištěna mobilita při vzájemném zastupování pracovníků. Zároveň se s tím zjednodušuje zálohování, protože je možné provádět jej centrálně na serveru, kde mají uživatelé svoje „profily“. Proces je jedním z klasických módů způsobů zpracování dat uživatele v doméně Microsoft. [36]

12.4 Zálohování produkčních databází úřadu práce

Zálohování databází v prostředí MPSV je do té míry rozsáhlou tématikou, že není možné ji plně postihnout. Proto se omezíme na zálohování databáze produktu OKpráce provozovaného na oddělení zaměstnanosti úřad práce. SQL databáze zaměstnanosti úřadu práce je součástí produktů OKpráce. Jeho historie sahá zpět až do roku 1997. Za tu dobu byla několikrát změněna verze databázového stroje. Vždy se jednalo o databázi Oracle. V současné době je průměrná velikost okresní databáze běžného venkovského okresu cca 10 GB. Velikost dislokovaného pracoviště téhož okresu bývá okolo 4 GB. Databáze Oracle umožňuje dva druhy zálohování. První druh je možné provozovat za chodu, tedy zároveň s činností

uživatelů. Tento nebyl pro značnou komplikovanost použit. Využívá se zálohování ve výhradním režimu databáze. Všichni uživatelé jsou odpojeni, připojen je pouze zálohovací klient. Tento klient postupně vyčítá všechny tabulky databáze a ukládá je do velkého souboru. Součástí tohoto souboru jsou nejen všechna data, která databáze uchovává, ale i údaje o uživatelích databáze, jejich přístupových právech a také vlastní parametry databáze. Takovýto export se nazývá úplným. Pokud jej pravidelně pořizujeme, jsme schopni obnovit databázi v plném rozsahu a to včetně všech přístupových hesel. Tento druh zálohy probíhá denně. Denní zálohy archivujeme minimálně po dobu jeden a půl cyklu trvání výplatního období. To znamená, že v každém okamžiku jsme schopni obnovit databázi do stavu před poslední výplatnou dávek, které úřad práce vyplácí. Tím je zajištěno, že je možno opakovat případný chybný výpočet způsobený objevením chyby po změně výpočetních algoritmů způsobených např. změnou zákona.

Fyzické umístění datových záloh databáze OKpráce podléhá předpisům o ochraně a nakládání s citlivými osobními údaji. Typickým médiem pro uchovávání datových záloh tohoto druhu jsou výměnné pevné disky případně disková pole. Pro zmenšení pravděpodobnosti ztráty dat při havárii datových médií probíhá ukládání na jednotlivá média cyklicky každý den na jiné. Média se prostřídávají např. každý druhý den je na jiném médiu nebo sudý a lichý týden. Další strategií pro zmenšení pravděpodobnosti ztráty dat je duplikace záloh na více různých míst. Tím se dosáhne ochrany před nenadálou živelnou pohromou nebo vyšší mocí. Pro případ vzniku takových událostí existuje evakuační plán. Archivní trezory, ve kterých jsou datová média ukládána, jsou zahrnuta do evakuačního plánu budovy. Pro případ zřícení budovy jsou umístěny tak, aby byly mimo zasypaný kužel.

Vadná zálohovací média a vadné datové disky z pracovních stanic nebo serverů podléhají při své likvidaci komisionálnímu postupu. Za přítomnosti jmenované komise je provedena fyzická likvidace diskových médií. Po provedení tohoto úkonu není médium čitelné ani částečně. Než k tomuto úkonu dojde, jsou tyto citlivé periferie uloženy stejně bezpečně jako například zálohovací média. [36]

13 VLIV SLOŽENÍ ZAMĚSTNANCŮ ÚP NA BEZPEČNOST ZPRACOVÁVANÝCH DAT

Personální úroveň zahrnuje několik druhů opatření. Jako první můžeme uvést postupy a činnosti, které vlastně nevyžadují výpočetní techniku jako takovou. Ty souvisí s právními aspekty pracovního poměru. Další oblastí je fyzická lokace a rozdělení kontaktních míst úřadů práce, jejich rozdělení na zóny podle přístupu apod.

Interakce zaměstnanců s prostředky výpočetní techniky začíná použitou výpočetní technikou (nezapomínejme na notebooky a PDA) zaměstnavatele, na připojení do sítě ve vlastní kanceláři případně Wi-Fi na pracovišti (PDA manažerů).

Nejtěsnější interakce s intranetem a počítačovou sítí pak přichází při přihlašování se ke koncové stanici a k jednotlivým aplikacím, které nese. Použití přihlašovací karty pak je vyšší úrovní přihlašování heslem. Zde je možno uložit i nastavení práv na jednotlivé aplikace obsažené v intranetu, tak další prvky zabezpečení. Například podpisové a šifrovací certifikáty pro e-mail a komunikaci.

13.1 Zabezpečení podmínkami pracovní smlouvy

Zaměstnanci MPSV mají jistý minimální stupeň povinné mlčenlivosti obsažen již v pracovní smlouvě. Jeho přesné znění je odsouhlaseno zaměstnavatelem, zástupcem odborů a odpovídá obvyklým standardům státní správy. Po dobu trvání pracovního poměru je trvale aktualizováno v souvislosti s aktuálními požadavky. V případě rozvázání pracovního poměru je uplatňována doložka o mlčenlivosti vůči budoucím zaměstnavatelům v přiměřené míře. Pracovní smlouva obsahuje termín nástupu, dobu PP (určitá, neurčitá), odvolává se na pracovní nebo služební poměr.

13.2 Zabezpečení oddělením klientské a obslužné zóny

Jednotlivá pracoviště úřadů práce mají prostory pro veřejnost. Jejich oddělení od služebních a obslužných prostor je zajištěno přepážkami a průchody. Přepážky jsou geometricky upraveny tak, aby nebylo možno neoprávněnou osobou odejmutí citlivých dokumentů. Průchody mezi oběma zónami mají evidovány osoby, které jimi mohou procházet. Toto je zajištěno jak elektronickými klíči, tak kódovanými mechanickými klíči s regulovaným přístupem.

13.3 Zabezpečení technickými prostředky HW pracovní stanice

Pracovní stanice úřadu jsou zabezpečeny na úrovni připojení k intranetové síti. Není možno provozovat neautorizovanou stanici. Tedy není technicky možno připojit neautorizovanou stanici do intranetu. Detaily jsou mimo rozsah této práce.

13.4 Zabezpečení technickými prostředky HW uživatele

Uživatel pro výkon činnosti získá čipovou kartu. Toto je prostředek vlastně na rozhraní mezi klasickými hesly a technickým prostředkem. Lze říci, že je to nosič hesel a zabezpečení. Je vydán plně personalizován s údaji a právy uživatele intranetu. Verze a stupeň zabezpečení odpovídá úrovni obvyklé v bankovním sektoru. Uživatel se autorizuje proti ověřující entitě intranetu. Správnost přístupového hesla je pravidelně kontrolována. V případě opětovného nesprávného zadání je heslo odstaveno. Je stanoven postup, jak je možné obnovit funkčnost. Postup zahrnuje ověření dalších specifických údajů pro obnovení, které se zaznamenají oproti databázi uživatelů.

13.5 Zabezpečení pomocí ověřování komunikace s aplikacemi

Jednotlivé aplikace, provozované jako součást intranetu, mají své vlastní ověřovací protokoly, kterými potvrzují každý úkon prováděný uživatelem. Jelikož toto ověření probíhá oproti údajům přihlášeného uživatele, lze i toto s výhradami považovat za personální ověření. Většina těchto postupů je inspirována a podobná postupům v bankovních systémech. Lze říci, že každou jednotlivou činnost informačních systémů prováděnou uživatelem, lze dohledat zpětně. A to jak v čase, tak v souslednosti činností.

13.6 Zabezpečení nekonfliktnosti úloh uživatele v aplikacích

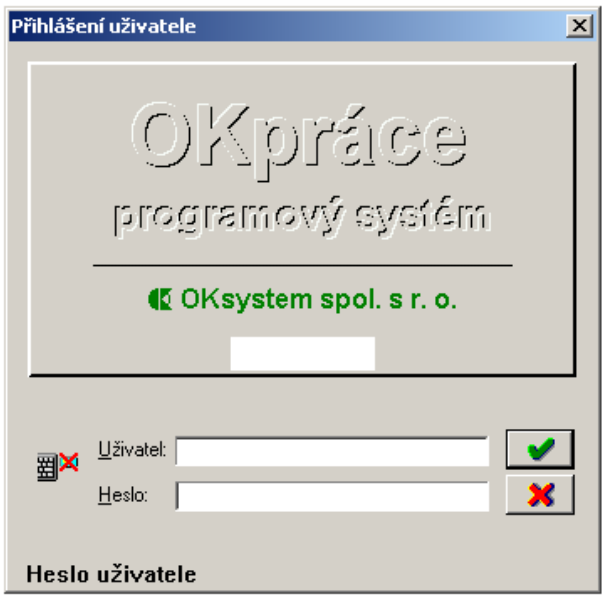
Při zavedení uživatele do jakékoliv aplikace intranetu je kontrolováno, zda je bezkonfliktní. To znamená, že uživatel aplikace nemá možnost osobního nebo cizího prospěchu z přidělené pozice v aplikaci. Materiální nebo finanční důsledky jednání uživatele, které by bylo možné považovat za podvodné či korupční, blokuje aplikace svou strukturou. Výjimky podléhají zvláštnímu schvalovacímu postupu včetně časového horizontu výjimky.

13.7 Zajištění datové bezpečnosti

V oblasti datové bezpečnosti se soustřeďujeme především na kontrolu přístupu do interní počítačové sítě a informačního systému.

13.7.1 Přístup do IS

Informační systémy ÚP sdílejí zabezpečení poskytované interní počítačovou sítí. Přístup k IS je zajištěn jménem a heslem alternativně kartou a pinem. Obě metody jsou rovnocenné. Údaje zaměstnance pro přihlášení se ověřují v databázi uživatelů IS. Tato databáze je unikátní a není připojena ani nijak nesouvisí s jinými přístupovými databázemi. Práva přístupu k jednotlivým modulům IS postihují činnosti prováděné zaměstnancem. Rozsah činností v prostoru (okres, část okresu) respektive času (třídění klientů např. podle data narození) jsou přiděleny nastavenými kategoriemi. Z důvodu zamezení vzniku klientelismu a případného zvýhodňování uchazečů o zaměstnání dochází k pravidelným změnám obsluhovaných oblastí nebo časových rozsahů. Tím se zajistí, že každý z klientů obdrží v několika letech vždy nového kontaktního pracovníka.



Obr. 27. Přihlášení uživatele IS [36]

V případě odchodu zaměstnance na dlouhodobou PN, mateřskou dovolenou nebo jiné dlouhodobé pozastavení činnosti je uživatel vyřazen. Jeho vyřazení je pouze logické. V systému zůstává zařazen, po jeho návratu dojde k nastavení stejných práv. Je tím zajištěna kontinuita prováděných úkonů na jednotlivých dokumentech uchazečů. V systému se předpokládá možná auditní činnost. Je zde možné zkontrolovat, zda pracovník například nevykonával činnost IS a zároveň čerpal nemocenské dávky, což může poukazovat na zneužití přihlašovacích údajů.

13.7.2 Přístup k všeobecným službám datové sítě ÚP

Jedná se zde především o komunikaci pomocí e-mailu a přístupu k službám webových stránek. E-mail je centrálně přidělován všem pracovníků dle definované struktury. E-mailová adresa je majetkem zaměstnavatele, je možno ji použít pouze ve služebním styku. Není povoleno jej použít pro účely soukromých aktivit. Služební e-mailové adresy jsou chráněny proti spamu a zneužití antivirovými systémy nasazenými na poštovních serverech. Nutný přístup k veřejnému internetu je filtrován pomocí specializovaného softwaru, který je nasazený na místech propojení úřadu práce s veřejným internetem. Zaměstnanec dle své kategorie získává rozsahy oprávnění, které se směrem k vedoucím pracovníkům zvyšuje. [36]

14 ANALÝZA RIZIK

Analýza rizik je provedena prostřednictvím bodové polokvantitativní metody „PNH“. Za pomoci této metody lze jednoduchým a přehledným způsobem vypočítat míru rizika použitím vzorce **R = P * N * H.**

Bodová metoda vyhodnocuje příslušné riziko ve třech složkách s ohledem na:

- **pravděpodobnost vzniku (P)** - odhadujeme zde pravděpodobnost, se kterou může nebezpečí nastat s vyžitím stupnice odhadu pravděpodobnosti vzestupně čísly 1 až 5,
- **pravděpodobnost následků (N)** - určuje závažnost nebezpečí, rovněž za pomocí stupnice čísel 1 - 5,
- **názor hodnotitelů (H)** - v této složce je zohledněna míra závažnosti rizika ohrožení, dynamičnost rizika, vliv pracovního prostředí a pracovních podmínek a další vlivy, které mají schopnost vyvolat potencionální riziko.

Bodové rozpětí vyjadřuje naléhavost úkolů přijetí opatření ke snížení rizika a prioritu bezpečnostních opatření. Při stanovení kategorie závažnosti vyhodnocených rizik je možné rozdělení do 5 rizikových stupňů:

- nepřijatelné riziko,
- nežádoucí riziko,
- mírné riziko,
- akceptovatelné riziko,
- bezvýznamné riziko.

Celkové hodnocení rizika lze pak následovně po stanovení jednotlivých činitelů získat součinem, jehož výsledkem je ukazatel míry rizika - **R.**

Tab. 2. Stanovení míry rizika [35]

Rizikový stupeň	R	Míra rizika
I.	> 100	Nepřijatelné riziko
II.	51 ÷ 100	Nežádoucí riziko
III.	11 ÷ 50	Mírné riziko
IV.	3 ÷ 10	Akceptovatelné riziko
V.	< 3	Bezvýznamné riziko

14.1 Analýza a vyhodnocení rizika

V následující tabulce jsou vedeny jednotlivé nejvýznamnější druhy činností úřadu práce spojené převážně se zpracováním osobních údajů uchazečů o zaměstnání, při kterých může dojít ke vzniku daného rizika. Dále je zde vyhodnocena závažnost rizika tvořená součinem jednotlivých hodnot P (pravděpodobnost vzniku), N (pravděpodobnost následků) a H (názoru hodnotitelů) s využitím stupnice čísel 1 - 5 vzestupně a nakonec navržená bezpečnostní opatření.

Tab. 3. Výpočet míry rizika s bezpečnostními opatřeními administrativního charakteru [35]

Druh činnosti	**Identifikace (zdroj) rizika**	**Vyhodnocení závažnosti rizika**				**Bezpečnostní opatření administrativního charakteru**
		P	**N**	**H**	**R**	
1. Kopírování předložených dokladů s osobními údaji občanů	Zneužití duplicitních dokladů uchazečů o zaměstnání	2	3	2	**12**	• zapojení technických prostředků při vytváření kopií (zavedení PINu do kopírovacích strojů, uložení náhledu k vytvořené kopii)
2. Vedení a ukládání fyzických spisů klientů	Odcizení či poškození fyzických spisů neoprávněnými osobami případně samotnými klienty	3	4	2	**24**	• vybavit kovové kartotéky zámky • přesunout aktuálně zpracovávanou dokumentaci z volně dostupných pořadníků na stolech odborných poradců do uzamykatelného uložiště

Tab. 4. Výpočet míry rizika s bezpečnostními opatřeními personálního charakteru [35]

Druh činnosti	**Identifikace (zdroj) rizika**	**Vyhodnocení závažnosti rizika**				**Bezpečnostní opatření personálního charakteru**
		P	**N**	**H**	**R**	
1. Vkládání osobních údajů občanů do informačního systému ÚP	Záměrné či neúmyslné vložení nesprávných údajů klienta do IS, záměna osob	4	4	1	**16**	• po přidělení IK (identifikačního kódu) občana neprodlené ověření údajů dle IK občana z kontrolního registru MPSV
2. Založení evidence úřadu práce na cizích pracovištích, nesehraní dat klienta ke dni nároku na dávku (vznik dvojí evidence)	Zneužití dávek úřadu práce, vznik duplicitní evidence	4	3	3	**36**	• ověřit možnou další evidenci občana při podezření na změnu trvalého bydliště
3. Zadání neadekvátního nejvyššího dosaženého vzdělání klienta	Nevhodnost nabízeného zaměstnání z hlediska nejvýše dosaženého vzdělání	4	4	2	**32**	• dodržovat kontrolu správnosti údajů v pravidelném cyklu
4. Zadání chybného oborového čísla vzdělání klienta	Nevhodnost nabízeného zaměstnání z hlediska oboru vzdělání klienta	4	5	2	**40**	• doplňovat správné vzdělání klienta dle čísla oboru uvedeného na předloženém dokladu o vzdělání • kontrola odpovědnými pracovníky
5. Zprostředkování nevhodného druhu zaměstnání vzhledem k praxi a dovednostem UoZ v IS	Laxní přístup zaměstnance, nezájem, demotivovanost	3	4	2	**24**	• proškolování zaměstnance pro dosažení správného rozhodnutí ve věci zprostředkování zaměstnání, • finanční odměna

Druh činnosti	Identifikace (zdroj) rizika	Vyhodnocení závažnosti rizika				Bezpečnostní opatření personálního charakteru
		P	**N**	**H**	**R**	
6. Zadávání zdravotního stavu klienta do IS ÚP dle lékařského potvrzení	Nesprávnost vyplněného zdravotního omezení uchazeče, nevyplněna pracovní rekomandace, zprostředkování nevhodného typu zaměstnání	3	2	1	**6**	• doplňovat zdravotní omezení klienta dle platného lékařského potvrzení • kontrola odpovědnými pracovníky
7. Převzetí lékařem vystavené dočasné neschopnosti klienta plnit si své povinnosti z důvodu nemoci nebo úrazu vůči ÚP a zadání do IS	Zneužití stavu práce neschopnosti, nedodržení režimu dočasné neschopnosti, maření zprostředkování zaměstnání	5	5	3	**75**	• kontrola ze strany úřadu práce v zákonem stanoveném rozsahu • proškolování zaměstnanců v oblasti dané problematiky
8. Ověřování výše platu klienta před nezaměstnaností	Uvedení neodpovídající (zpravidla) vyšší částky příjmu pro výpočet PvN	3	3	2	**18**	• kontrola mzdové účtárny zaměstnavatele za pomoci finančního úřadu a úřadu práce
9. Kontrola místa a způsobu výplaty dávek	Záměrná či nahodilá záměna klienta (chyba čísla účtu)	2	3	1	**6**	• doložení výpisu vlastnictví z dané banky klienta • eliminace výplat dávek složenkou
10. Vyplácení dávky podpory v nezaměstnanosti (PvN) z IS ÚP	Nepozastavení výplaty dávek PvN z důvodu zákonné překážky, nenahlášení výkonu NZ klientem	3	4	3	**36**	• zadání činnosti klienta na základě doloženého pracovněprávního dokladu • kontrola správnosti zadaného NZ odpovědným pracovníkem • finanční odměna

Druh činnosti	**Identifikace (zdroj) rizika**	**Vyhodnocení závažnosti rizika**				**Bezpečnostní opatření personálního charakteru**
		P	**N**	**H**	**R**	
11. Jednání s problémovým a agresivním klientem	Slovní či fyzické napadení zaměstnance ÚP	4	4	3	**48**	• zavedení povinných kurzů sebeobrany ve spolupráci s Policií ČR
12. Doručování písemností prostřednictvím datové schránky klienta	Nedoručitelnost písemnosti z důvodu chybně zadaných znaků datové adresy klienta	1	2	1	**2**	• kontrola kontaktních údajů klienta z kontrolního registru MPSV • aktualizace kontaktních údajů při pravidelných schůzkách s klienty
13. Doručování písemností klientům prostřednictvím České pošty	Nedoručitelnost písemnosti z důvodu nenahlášení změny trvalého bydliště občanem v zákonem stanovené lhůtě, neuvedení nové doručovací adresy (v případě, že není totožná s TB)	5	5	3	**75**	• při zjištění neshody adresy občana v IS s adresou v kontrolním registrem MPSV vyzvat uchazeče k nahlášení aktuální platné adresy • ověřit údaje klienta dle platného občanského průkazu, případně náhradního úředního dokladu
14. Odpovídání na dotazy týkajících se klientů státním orgánům (soudy, OSSZ, Policie ČR aj.) datovou schránkou	Nedoručitelnost písemnosti z důvodu nesprávnosti datové schránky orgánu, záměna datových schránek	2	1	1	**2**	• kontrola odpovědného vedoucího zaměstnance o správnosti doručení písemnosti

Tab. 5. Výpočet míry rizika s bezpečnostním opatřením z hlediska logické bezpečnosti [35]

Druh činnosti	**Identifikace (zdroj) rizika**	**Vyhodnocení závažnosti rizika**				**Bezpečnostní opatření z hlediska logické bezpečnosti**
		P	**N**	**H**	**R**	
1. Vystavování potvrzení týkající se předchozích evidencí klienta	Nedostupnost požadovaných údajů (za účelem doložení sociálního či zdravotního pojištění UoZ)	3	2	1	**6**	• zvýšení přístupnosti k požadovaným informacím z předchozího ISÚP (90. léta) pomocí udělení přístupového práva

Tab. 6. Výpočet míry rizika s bezpečnostním opatřením z hlediska datové bezpečnosti [35]

Druh činnosti	**Identifikace (zdroj) rizika**	**Vyhodnocení závažnosti rizika**				**Bezpečnostní opatření z hlediska datové bezpečnosti**
		P	**N**	**H**	**R**	
1. Přihlašování se do OS a IS prostřednictvím čipové karty zaměstnance	Odcizení čipové karty neoprávněnou osobou, poškození identifikační karty	3	3	3	**27**	• uschování čipové karty do příručního uzamykatelného kontejneru při každém odhlášení z počítače, (konec pracovní doby, odchod na polední přestávku)

Tab. 7. Výpočet míry rizika s bezpečnostním opatřením z hlediska fyzické bezpečnosti [35]

Druh činnosti	**Identifikace (zdroj) rizika**	**Vyhodnocení závažnosti rizika**				**Bezpečnostní opatření z hlediska fyzické bezpečnosti**
		P	**N**	**H**	**R**	
1. Vstup do prostor KoP Kyjov stávajícím způsobem (PIN + kláves. zkratka)	Neoprávněné vniknutí do objektu, zneužití osobních údajů klientů	2	3	3	**18**	• zavedení biometrické metody (čtečka otisku prstu) k oprávněnému přístupu do objektu

Z výše uvedených tabulek vyplývá, že na úřadu práce jsou prováděny takové činnosti, při kterých jsou identifikována 2 bezvýznamná rizika, 3 akceptovatelná rizika, 12 mírných rizik a 2 rizika nežádoucí. Z provedené analýzy nebylo zjištěno žádné nepřijatelné riziko. Nežádoucí rizika vyplývají především z toho důvodu, že jejich zdroj plyne zejména z pochybení samotných klientů a nikoli zaměstnanců úřadu práce.

V ostatních případech je nejvýznamnějším bezpečnostním opatřením nepřetržitá pravidelná kontrola při nakládání s osobními údaji klientů v informačním systému úřadu práce jak ze strany přepážkových zaměstnanců, kteří jsou odpovědní za správnost a věcnost ručně zadávaných údajů klientů, tak ze strany dalších oprávněných osob, jejichž cílem je zejména kontrola činností samotných zprostředkovatelů z hlediska fyzické i elektronické podoby spisu. Na již nepravdivé údaje (změna příjmení, změna trvalého bydliště klienta aj.) upozorňuje přímo kontrolní registr MPSV v ISÚP a je nezbytně nutné, aby zaměstnanci na tyto změny reagovaly v co nejkratším časovém horizontu.

Co se týče zabezpečení přístupu do IS a samotných prostor KoP Kyjov je nutné dbát bezpečnostních opatření bránících odcizení či poškození identifikačních předmětů zaměstnanců a zavedení možných inovačních metod vedoucích ke zvýšení bezpečnosti objektu.

15 CELKOVÉ ZHODNOCENÍ INFORMAČNÍHO SYSTÉMU ÚŘADU PRÁCE

Zkoumaný informační systém je optimálním ISVS. Z důvodu jasné hierarchie jednotlivých databází a centrálního datového střediska je informační systém velmi dobře zorganizován. Výhodou je užití levných datových linek, nevýhodou je naopak dlouhá doba zpracování dat, což má za následek vyšší finanční náročnost. Co se týče antivirové ochrany a procesů zálohování dat je IS zabezpečen na odpovídající vysoké úrovni jak softwarovým tak hardwarovým vybavením včetně vysoké profesionality odpovědných informačních pracovníků.

Pro uživatele je tento ISVS velmi srozumitelně a logicky řešen. Jednotlivé úkony spojené se zadáváním osobních údajů občanů na sebe vzájemně navazují a umožňují tak jednoduchou uživatelskou obsluhu s možností rychlého vložení a opravy dat. Aktuálnost dat klientů je též kontrolována centrálním registrem MPSV, což výrazně napomáhá k včasné identifikaci vzniklých změn a chybně zadaných osobních údajů klientů k jejich neprodlené opravě uživateli informačního systému.

Výhodou zmíněného IS je též možnost rychlého vyhledávání konkrétních klientů úřadu práce z hlediska požadovaných kritérií, ať už z hlediska pohlaví, bydliště, nejvýše dosaženého vzdělání a oboru vzdělání, zdravotního stavu či požadavků na zaměstnání, tak co se týče délky evidence ve dnech či dle data podání samotné žádosti o zprostředkování zaměstnání nebo podpory v nezaměstnanosti klientem za účelem zprostředkování vhodného zaměstnání.

Z analýzy rizik jednotlivých činností provozovaných při nakládání s osobními údaji klientů jasně vyplývá, že rizika z nich plynoucí jsou v převážné míře vyhodnocena jako rizika akceptovatelná. Nejobávanější rizika, při nichž by mohlo dojít k selhání podstaty informačního systému, tj. především vyplacení oprávněné dávky, je způsobeno chybou samotných klientů při neuvedení důležitých změn majících vliv na hladký průběh plateb vyplácených úřadem práce v pravidelném měsíčním cyklu. Informační systém jako takový je nastaven fungujícím systémem bez potřeb revitalizace jeho funkčnosti či potřeb zavedení nových inovací.

16 NAVRŽENÁ OPATŘENÍ

Níže uvedená navržená opatření jsou rozdělena dle jednotlivých úrovní zabezpečení.

16.1 Administrativní úroveň zabezpečení

Při získávání osobních údajů občanů z kopií předložených originálů navrhuji zapojení technických prostředků do kopírovacích zařízení za účelem zvýšení bezpečnosti. Jedná se o povinné zadávání PIN kódu při obsluze stroje, dále ukládání náhledů vytvořených kopií v délce jednoho měsíce.

Příruční archívy tvořené kovovými kartotékami u jednotlivých přepážek je nutné vybavit zámky, které zapříčiní to, aby nebylo možné se spisy klientů nekontrolovatelně manipulovat. Klíč bude vlastnit pouze pracovník dané přepážky a vedoucí zaměstnanec. Navrhuji též, aby veškerá další dokumentace, která je uložena v pořadnících na stolech zaměstnanců, byla přesunuta do uzamykatelného uložiště a nebyla tak volně dostupná s možností zneužití.

16.2 Personální úroveň zabezpečení

Vzhledem k tomu, že odpovědnost za správnost zadávaných údajů klientů do informačního systému úřadu práce nesou v převážné míře sami zaměstnanci, je nutná neustálá kontrola, tzv. zpětná vazba, provedených úkonů jak samotnými pracovníky přepážky tak odpovědnými vedoucími zaměstnanci.

Pracovníci jsou proškolováni, co se týče novel zákonů a nařízení v pravidelných cyklech. Absolvují i další volitelná školení za účelem osvojení nových dovedností například při jednání s problémovými klienty, zvládání stresových situací, v případě již projeveného syndromu vyhoření, které má za následek snížení pracovní produktivity, pak zregenerování sebe sama v rámci kolektivních uvolňujících sezení za pomoci vyškolených odborníků.

Zaměstnanci jsou motivováni zejména finanční odměnou za dobře odvedenou práci. V případě, že u pracovníka za kalendářní čtvrtletí nebude zjištěno žádné závažné pochybení, které by mělo za následek například nevyplacení dávky náležící klientovi z důvodu neodsouhlasení nároku nebo naopak způsobení přeplatku dávky pro nepozastavení nároku ze zákonného důvodu, který uchazeč byť nahlásil, ale zaměstnanec pochybil při jeho zpracování, bude zaměstnanci náležet finanční odměna ve výši 3 000,- Kč vyplatitelná vždy po uplynutí sledovaného čtvrtletí.

Dalším navrženým opatřením je zavedení povinných kurzů sebeobrany alespoň v základní úrovni. Jelikož v současné době roste počet agresivních klientů a bohužel množících se slovních i fyzických útoků na úředníky, je prevence v této oblasti z mého pohledu nutností. Do zavedeného programu sebeobrany by byli zapojeni jako školitelé policisté ČR.

16.3 Logická úroveň zabezpečení

Jelikož současný ISÚP není původním IS, je nutné zajistit dostatečnou obsluhu i předchozího informačního systému za účelem vystavení potvrzení občanům, kteří byli v minulých letech evidováni na úřadu práce, a to za pomoci uděleného přístupového práva informatikem konkrétním proškoleným osobám z řad zaměstnanců ÚP. Toto požadované potvrzení slouží především k prokázání sociálního či zdravotního pojištění klienta v době nezaměstnanosti.

16.4 Datová úroveň zabezpečení

V rámci bezpečnostního opatření je nutné, aby všichni zaměstnanci uschovávali svoji čipovou kartu pro přihlášení k operačnímu i informačnímu systému do příručního uzamykatelného kontejneru, který má každý zaměstnanec k dispozici v bezprostřední blízkosti svého pracoviště, při každém odhlášení z počítače, obzvláště pak s koncem pracovní doby či pouze při odchodu na polední přestávku. Tato povinnost bude kontrolována v pravidelných i náhodných intervalech odpovědnými vedoucími pracovníky.

16.5 Fyzická úroveň zabezpečení

Co se týče možnosti zvýšení fyzické úrovně bezpečnosti, navrhuji zabezpečení přístupu do prostor kontaktního pracoviště v Kyjově pomocí čtečky otisku prstu bez nutnosti použití klíče. Pro běžné uživatele zde budou nainstalována časová okna, ve kterých budou zaměstnanci oprávněni dveře odemknout, dále by systém vedl i docházku jednotlivých zaměstnanců. V případě pokusu o neoprávněný vstup je takovéto zařízení vybaveno signalizací poplachového výstupu, která je napojena na pult centralizované ochrany. Tento jedinečný prvek tak bezpodmínečně zvýší zabezpečení chráněného objektu před nežádoucím vniknutím s cílem zneužití osobních údajů občanů.

ZÁVĚR

Ve své diplomové práci jsem se zabývala systémem zabezpečení ochrany osobních údajů občanů v informačním systému veřejné správy, konkrétně na úřadu práce, kde pracuji a z tohoto důvodu je mi tato problematika velice blízká. Cílem práce bylo tedy zhodnotit současný stav zabezpečení osobních údajů a navrhnout vhodný způsob implementace ochranných mechanismů ke zvýšení bezpečnosti.

Obsah teoretické části se zabýval zejména problematikou bezpečnosti a popisem informačního systému veřejné správy obecně od jeho vzniku až po ukončení činnosti. Dále jsou zde uvedeny základní právní předpisy a to zejména zákon č. 365/2000 Sb. o informačních systémech veřejné správy a další normy související s řízením bezpečnosti informací. Další kapitola je věnována teorii analýzy rizik informačních systémů z hlediska přístupů. Předposlední kapitola se zabývá samotným ohrožením informačního systému a popisem jednotlivých hrozeb. Poslední kapitola pak řeší možnosti zabezpečení informačního systému z hlediska jednotlivých úrovní bezpečnosti.

V úvodu praktické části jsem představila analyzovaný prvek státní správy a to kontaktní pracoviště Úřadu práce v Kyjově, jak z hlediska věcného tak fyzického uspořádání. Dále jsem se zabývala podstatnými aspekty informační a spisové bezpečnosti úřadu s následným stručným popisem základních pracovních postupů v oblasti podání žádosti o zprostředkování zaměstnání a podpory v nezaměstnanosti. Další díl je věnován samotnému informačnímu systému úřadu práce, jakožto jeho struktuře, antivirové ochraně, procesu zálohování dat a vlivu složení zaměstnanců na bezpečnost zpracovaných dat. Následně je zde zpracována analýza rizik jednoduchou bodovou metodou s výslednými navrženými opatřeními, které přispějí ke zvýšení bezpečnosti osobních údajů občanů.

SEZNAM POUŽITÉ LITERATURY

[1] JAŠEK, Roman. *Ochrana znalostí a dat v podnikových informačních systémech.* Zlín: Univerzita Tomáše Bati, Fakulta managementu a ekonomiky, 2002, 115 s. ISBN 807-31-8095-2.

[2] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management III.* Zlín: Radim Bačuvčík - VeRBuM, 2013. ISBN 978-80-87500-35-4.

[3] Veřejná správa. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001, 2017 [cit. 2017-11-03]. Dostupné z: https://cs.wikipedia.org/wiki/Veřejná_správa

[4] Metodické pokyny: Co je a co není ISVS. *Ministerstvo vnitra České republiky* [online]. 2009 [cit. 2017-11-3]. Dostupné z: http://www.mvcr.cz/clanek/co-je-a-co-neni-isvs.aspx

[5] JAŠEK, Roman, Miroslava DOLEJŠOVÁ a Pavel ROSMAN. *Informační technologie ve veřejné správě.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 183 s. ISBN 978-80-7318-607-4.

[6] Legislativa: Zákon č. 365/2000 Sb., o informačních systémech veřejné správy. *Ministerstvo vnitra České republiky* [online]. 2016 [cit. 2017-11-03]. Dostupné z: http://www.mvcr.cz/clanek/legislativa-zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy.aspx

[7] Zákon o informačních systémech veřejné správy. *In: 365/2000 Sb.* 2000.

[8] ZBYTOVSKÝ, Jaroslav. *GDPR*. Úřad práce ČR, 2018.

[9] *Řízení bezpečnosti informací* [online]. Praha 4: Risk Analysis Consultants, 2015 [cit. 2017-11-11]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/BS7799/$FILE/RAC%20ISMS_Datasheet_CZ_151210.pdf

[10] ISMS: normy ISO 27001 a ISO 27002. *Risk Analysis Consultants* [online]. 2017 [cit. 2017-11-11]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/BS7799

[11] SMEJKAL, V., RAIS, K. *Řízení rizik ve firmách a jiných organizacích.* 3. Vyd. Praha: Grada Publishing, a.s., 2010. 360 s. ISBN 978-80-247-3051-6.

[12] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management V*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-67-5.

[13] ALINČOVÁ, Lenka a Jitka VOŘÍŠKOVÁ. *Bezpečnostní politika IS: Městská část Praha – Kunratice 2015 - 2020* [online]. Praha, 2015 [cit. 2017-11-20]. Dostupné z: https://www.praha-kunratice.cz/sites/default/files/smernice/04_bezpecnostni_politika.pdf

[14] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM.* 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

[15] Informační bezpečnost - její klíčové aspekty, hrozby a minimalizace rizika. *Wikisofia* [online]. 2013 [cit. 2017-11-20]. Dostupné z: https://wikisofia.cz/wiki/Informační_bezpečnost_-_její_klíčové_aspekty,_hrozby_a_minimalizace_rizika#cite_note-5

[16] POŽÁR, *Josef. Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s. Vysokoškolské učebnice. ISBN 80-86898-38-5.

[17] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[18] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat.* Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.

[19] Počítačový vir. *IT SLOVNÍK.cz* [online]. 2008 [cit. 2017-12-04]. Dostupné z: https://it-slovnik.cz/pojem/pocitacovy-vir

[20] HEINIGE, Karel. *Viry a počítače.* Praha: Mobil Media, 2001. PC World edition. ISBN 808-65-9302-9.

[21] PEŠA, Radim. *Počítačové viry* [online]. [cit. 2017-12-21]. Dostupné z: http://ics.muni.cz/bulletin/articles/160.html

[22] Počítačový červ. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2017-12-21]. Dostupné z: https://cs.wikipedia.org/wiki/Počítačový_červ

[23] JALŮVKA, Josef. *Moderní počítačové viry: podstata, prevence, ochrana.* 2. aktualiz. vyd. Praha: Computer Press, 2000. Všechny cesty k informacím. ISBN 80-7226-402-8.

[24] Co je to trojské koně a jak je odstranit. *Odstranit virus* [online]. 2016 [cit. 2017-12-21]. Dostupné z: https://odstranitvirus.cz/trojske-kone/

[25] Co je hoax. *E bezpečí* [online]. 2008 [cit. 2017-12-21]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/hoax-spam/91-25

[26] KOCMAN, Rostislav a Jakub LOHNISKÝ. *Jak se bránit virům, spamu, dialerům a spyware.* Brno: CP Books, 2005. ISBN 80-251-0793-0.

[27] PETERKA, Jiří. Uznávaný, nebo jen zaručený elektronický podpis? *Computerworld* [online]. **2012**(3) [cit. 2018-01-02]. Dostupné z: http://www.earchiv.cz/b12/gifs/b0209102.png

[28] Zálohová dat. *Chytrý Software* [online]. 2011 [cit. 2018-01-02]. Dostupné z: http://www.chytrysoftware.cz/sprava-dat/zaloha-dat.php

[29] Aktualizace (software). In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-01-02]. Dostupné z: https://cs.wikipedia.org/wiki/Aktualizace_(software)

[30] Zabezpečte svá hesla. *Google centrum pro bezpečnost* [online]. [cit. 2018-01-02]. Dostupné z: https://www.google.cz/intl/cs/safetycenter/everyone/start/password/

[31] Antivirová ochrana. *Bezpečný internet.cz* [online]. [cit. 2018-01-02]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/zabezpeceni-pocitace/antivirova-ochrana.aspx

[32] MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. *Hacking bez záhad.* Praha: Grada, 2007. ISBN 978-80-247-1502-5.

[33] JAŠEK, Roman a Martin LUKÁŠ. *Informatika ve veřejné správě.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2003. ISBN 80-7318-147-9.

[34] Organizační struktura Úřadu práce České republiky. *Úřad práce České republiky* [online]. [cit. 2018-04-19]. Dostupné z: http://portal.mpsv.cz/upcr/gr/orgstr

[35] Zdroj vlastní

[36] Zdroj interní

[37] What is Windows Defender? *Microsoft* [online]. [cit. 2018-04-25]. Dostupné z: https://www.microsoft.com/en-us/safety/pc-security/windows-defender.aspx

[38] UrBackup – instalace a konfigurace. *Napovedy.cz* [online]. [cit. 2018-04-23].

[39] Instalace klienta. *Www.SAMURAJ-cz.cz* [online]. [cit. 2018-04-23]. Dostupné z: https://www.samuraj-cz.com/clanek/sccm-2012-instalace-klientu-zamereno-na-client-push/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ČR	Česká republika
ČSN	Česká technická norma
DDOS	Distributed denial of service
ESF	Evropský sociální fond
GDPR	General data protection regulation
IEC	International Electrotechnical Commission
IK	identifikátor
IS	Informační systém
ISMS	Systém řízení bezpečnosti informací
ISO	International Organization for Standardization
ISVS	Informační systém veřejné správy
KoP	Kontaktní pracoviště
KRK	Kontrolní registr Ministerstva práce a sociálních věcí
MPSV	Ministerstvo práce a sociálních věcí
NZ	nekolidující zaměstnání
OECD	Organisation for Economic Co-operation and Development
OSSZ	Okresní správa sociálního zabezpečení
PDA	Personal digital assistant
PDCA	plan-do-check-act
PGP	Pretty Good Privacy
PN	pracovní neschopnost
PNO	počet nezaměstnaných osob
PvN	podpora v nezaměstnanosti
SCCM	System Center Configuration Manager

SQL	databázové prostředí od společnosti Microsoft
SSP	Státní sociální podpora
TB	trvalé bydliště
UoZ	uchazeč o zaměstnání
ÚP	Úřad práce
WAN	Wide Area Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ŽÁDOST O ZPROSTŘEDKOVÁNÍ ZAMĚSTNÁNÍ

ÚŘAD PRÁCE ČR

ZAM
UCHAZEČ – EVIDENCE

Záznam o dni podání žádosti:

OSÚ
S 15

Žádost o zprostředkování zaměstnání

§ 26 odst. 1 zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů (dále jen „zákon o zaměstnanosti")

A. Žadatel:

Příjmení:	Jméno[1]:	Rodné číslo v ČR[2]:
Rodné příjmení[3]:	Titul před: za:	Státní občanství:
Místo narození[4]:		
Bydliště[5]: Obec: ..... Část obce:		
Ulice: ..... Č. p.[6]: ..... Č. orient.: ..... PSČ:		
Adresa pro doručování v ČR[7]: Obec: ..... Část obce:		
Ulice: ..... Č. p.[6]: ..... Č. orient.: ..... PSČ:		
Telefon:	E-mail:	

B. Naposledy jsem byl(a) veden(a) v evidenci uchazečů o zaměstnání:

Úřad práce: Stát:

C. Poslední ukončená činnost před podáním této žádosti:

☐ zaměstnání	☐ samostatná výdělečná činnost	☐ jiná výdělečná činnost	☐ náhradní doba zaměstnání[8]	☐ jiná činnost	
Název profese:					
Název zaměstnavatele nebo druh činnosti:			Datum skončení:		
V době 3 pracovních dnů před podáním této žádosti jsem byl(a) v pracovní neschopnosti:			☐ ano	☐ ne	

1) Uveďte všechna jména osoby.

2) Cizinci, pokud nemají v ČR přiděleno rodné číslo, uvedou v kolonce **Rodné číslo v ČR** datum narození ve tvaru den, měsíc, rok a pohlaví ve tvaru: M nebo Ž (muž nebo žena).

3) Kolonku **Rodné příjmení** vyplňte pouze v případě, že se liší od příjmení.

4) Vyplňte, nebylo-li Vám přiděleno rodné číslo.

5) Za bydliště se považuje:
- u státního občana ČR adresa místa trvalého pobytu na území ČR,
- u cizince, který je občanem EU nebo jeho rodinným příslušníkem anebo rodinným příslušníkem občana ČR, adresa trvalého nebo přechodného pobytu na území ČR, a pokud takový pobyt nemá, adresa místa, kde se na území ČR obvykle zdržuje,
- u cizince, který není občanem EU ani jeho rodinným příslušníkem ani rodinným příslušníkem občana ČR, adresa místa trvalého pobytu na území ČR, je-li držitelem modré karty, adresa uvedená jako místo pobytu v agendovém informačním systému cizinců.

6) Pokud je místo čísla popisného přiděleno číslo evidenční, uveďte před číslem písmeno E.

7) Nevyplňujte, pokud je adresa shodná s adresou bydliště.

8) **Za náhradní dobu zaměstnání se považuje doba** přípravy osoby se zdravotním postižením k práci, doba pobírání plného invalidního důchodu pro invaliditu třetího stupně, doba osobní péče o dítě ve věku do 4 let a doba osobní péče o fyzickou osobu mladší 10 let, která se podle zákona o sociálních službách považuje za osobu závislou na pomoci jiné fyzické osoby ve stupni I (lehká závislost). Dále doba osobní péče o fyzickou osobu, která se podle zákona o sociálních službách považuje za osobu závislou na pomoci jiné fyzické osoby ve stupni II (středně těžká závislost), ve stupni III (těžká závislost) nebo ve stupni IV (úplná závislost), pokud s uchazečem o zaměstnání trvale žije a společně uhrazují náklady na své potřeby; tyto podmínky se nevyžadují, jde-li o osobu, která se pro účely důchodového pojištění považuje za osobu blízkou. Za náhradní dobu se rovněž považuje doba výkonu dlouhodobé dobrovolnické služby na základě smlouvy dobrovolníka s vysílající organizací, která byla udělena akreditace Ministerstvem vnitra, nebo výkonu veřejné služby na základě smlouvy o výkonu veřejné služby, pokud rozsah vykonané služby překračuje v průměru alespoň 20 hodin v kalendářním týdnu a dále doba trvání dočasné pracovní neschopnosti nebo nařízené karantény osoby po skončení výdělečné činnosti, která zakládala její účast na nemocenském pojištění podle zákona o nemocenském pojištění, pokud si tato osoba nepřivodila dočasnou pracovní neschopnost úmyslně a pokud tato dočasná pracovní neschopnost nebo nařízená karanténa vznikla v době této výdělečné činnosti nebo v ochranné lhůtě podle zákona o nemocenském pojištění.

Tisk: Moraviapress, s.r.o. Břeclav – vzor 2017

17 08 01 806

D. Údaje o kvalifikaci:

Nejvyšší dosažené vzdělání (např. základní, střední vyučen, střední s maturitou, vyšší odborné, vysokoškolské):

Přehled absolvovaných škol:

Název školy (včetně učiliště)	Obor

Absolvovaná rekvalifikace a její zaměření (neuvádějte rekvalifikace zajištěné krajskou pobočkou ÚP ČR):

Odborné dovednosti[9]:

Jazykové znalosti:

Jazyk	Úroveň (aktivně/pasivně)	Jazyk	Úroveň (aktivně/pasivně)

E. Získané pracovní zkušenosti:

Uveďte povolání (název) vykonávaná 6 měsíců a déle	Délka výkonu povolání

F. Požadavky na zaměstnání:

Profese (uveďte profesi odpovídající Vašim znalostem, schopnostem a kvalifikaci):

Název

Ostatní požadavky:

Směnnost:	Úvazek:
Ubytování:	Mimo okres bydliště:
V zahraničí:	Jiné:

9) Uveďte např. řidičský průkaz včetně skupiny, znalost práce s PC, práce s kovem - řezání, pájení, svařování včetně zkoušky, obsluha technických zařízení - topičský průkaz, obsluha zemědělských strojů, obsluha stavebních strojů, poskytování služeb - plavčík, cvičitel apod., oprávnění podle vyhl. č. 50/1978 Sb., zdravotní průkaz, zbrojní průkaz a jiné.

Tisk: Moraviapress, s.r.o. Břeclav – vzor 2017

17 08 01 806

G. Zdravotní omezení související se zprostředkováním zaměstnání:

Zaškrtněte jednu z uvedených možností. Pokud zvolíte druhou možnost, upřesněte ji v dalších volbách.

☐ nemám zdravotní omezení

☐ mám zdravotní omezení – jsem:

- ☐ invalidní ve třetím stupni a schopen(a) výdělečné činnosti za zcela mimořádných podmínek (§ 39 odst. 4 písm. f) zákona č. 155/1995 Sb., o důchodovém pojištění, ve znění pozdějších předpisů)[10]
- ☐ invalidní ve druhém stupni (§ 39 odst. 2 písm. b) zákona o důchodovém pojištění)[11]
- ☐ invalidní v prvním stupni (§ 39 odst. 2 písm. a) zákona o důchodovém pojištění)[11]
- ☐ zdravotně znevýhodněnou osobou[12]
- ☐ osobou, které byla odejmuta invalidita v posledních 12 měsících

☐ mám jiná zdravotní omezení[13]

Zde uveďte konkrétní zdravotní omezení (např. nemohu pracovat ve výškách apod.):

H. Děti do 15 let v péči žadatele:

Příjmení	Jméno	Datum narození	Příjmení	Jméno	Datum narození

I. Jiná omezení související se zprostředkováním zaměstnání:

J. Osvědčení skutečností rozhodných pro zařazení a vedení v evidenci uchazečů o zaměstnání:

Čestně prohlašuji, že ke dni podání této žádosti

1. ☐ jsem ☐ nejsem **v pracovněprávním vztahu** (tj. pracovní poměr, vztah na základě dohody o pracovní činnosti a dohody o provedení práce) nebo **ve služebním poměru,**

   Pokud zvolíte první možnost, upřesněte ji v dalších volbách.

   ☐ pracovní - služební poměr ☐ dohoda o pracovní činnosti ☐ [redacted]

U zaměstnavatele:
Výše měsíčního výdělku (měsíční odměny):

2. ☐ jsem ☐ nejsem výdělečně činný(á) v cizině (pokud ano, uveďte stát) ____

3. **nejsem osobou samostatně výdělečně činnou** v České republice ani v cizině (za OSVČ v ČR se považuje fyzická osoba uvedená v § 9 zákona č. 155/1995 Sb., o důchodovém pojištění),

---

10) Dokládá se posudkem, potvrzením nebo rozhodnutím orgánu sociálního zabezpečení. Za fyzickou osobu, která je invalidní ve třetím stupni a je schopna výdělečné činnosti za zcela mimořádných podmínek, se považuje od 1. 1. 2010 též fyzická osoba, která byla ke dni 31. 12. 2009 plně invalidní podle § 39 odst. 1 písm. b) zákona č. 155/1995 Sb., o důchodovém pojištění.

11) Dokládá se posudkem, potvrzením nebo rozhodnutím orgánu sociálního zabezpečení. Částečná invalidita, která trvá ke dni 31. 12. 2009, se považuje od 1. 1. 2010 za invaliditu druhého stupně, byl-li důvodem částečné invalidity pokles schopnosti soustavné výdělečné činnosti nejméně o 50 %, a za invaliditu prvního stupně v ostatních případech.

12) Dokládá se potvrzením nebo rozhodnutím orgánu sociálního zabezpečení, rozhodnutím Úřadu práce ČR o uznání zdravotně znevýhodněnou osobou.

13) Dokládá se posudkem ošetřujícího lékaře (§ 21 zákona o zaměstnanosti).

Tisk: Moraviapress, s.r.o. Břeclav – vzor 2017

17 08 01 806

4. ☐ jsem[14] ☐ nejsem

a) společníkem společnosti s ručením omezeným,
b) jednatelem společnosti s ručením omezeným,
c) komanditistou komanditní společnosti,
d) členem představenstva nebo správní rady nebo statutárním ředitelem akciové společnosti,
e) členem dozorčí rady obchodní společnosti,
f) členem družstva,
g) ředitelem obecně prospěšné společnosti,
h) vedoucím organizační složky zahraniční právnické osoby,
i) fyzickou osobou pověřenou obchodním vedením

Název společnosti:

5. ☐ jsem[14] ☐ nejsem

a) nuceným správcem anebo správcem podle zvláštního právního předpisu (např. podle insolvenčního zákona),
b) likvidátorem,
c) prokuristou

Název zaměstnavatele/název seznamu, ve kterém jsem veden(a):

6. **nejsem členem zastupitelstva územního samosprávného celku**, kterému jsou vypláceny odměny jako členům zastupitelstev územních samosprávných celků, kteří tyto funkce vykonávají jako uvolnění členové,
7. **nejsem pěstounem, kterému je vyplácena odměna pěstouna** podle § 47j odst. 1 písm. c) a d) zákona o sociálně-právní ochraně dětí (20 nebo 24 tisíc Kč měsíčně),
8. ☐ jsem ☐ nejsem studentem denního studia na střední škole, konzervatoři, vyšší odborné škole, jazykové škole s právem státní jazykové zkoušky a prezenčního studia na vysoké škole,
9. **nejsem v dočasné pracovní neschopnosti**,
10. **nepobírám peněžitou pomoc v mateřství / jsem 6 týdnů po porodu**,
11. ☐ jsem ☐ nejsem **invalidní ve třetím stupni** podle § 39 odst. 2 písm. c) zákona č. 155/1995 Sb., o důchodovém pojištění, ve znění pozdějších předpisů,
12. **nevykonávám trest odnětí svobody**, nevykonávám **ochranné opatření zabezpečovací detenci, nejsem ve vazbě**,
13. **nejsem** soudcem, poslancem nebo senátorem Parlamentu, poslancem Evropského parlamentu, prezidentem, viceprezidentem nebo členem Nejvyššího kontrolního úřadu, Veřejným ochráncem práv nebo zástupcem veřejného ochránce práv, členem Rady pro rozhlasové a televizní vysílání, členem Rady Ústavu pro studium totalitních režimů, členem Rady Energetického regulačního úřadu nebo členem Rady Českého telekomunikačního úřadu, finančním arbitrem nebo zástupcem finančního arbitra, předsedou nebo místopředsedou Rady Národního akreditačního úřadu pro vysoké školství.

K. Potvrzuji, že:

1. nejsem veden(a) v evidenci uchazečů o zaměstnání v ČR,
2. ☐ jsem ☐ nejsem veden(a) v evidenci uchazečů o zaměstnání v jiném státě Evropské unie/EHP/Švýcarsku (pokud ano, uveďte stát)
3. jsem byl(a) poučen(a) o podmínkách zařazení a vedení v evidenci uchazečů o zaměstnání, o právech a povinnostech uchazeče o zaměstnání a o podmínkách nároku na podporu v nezaměstnanosti,
4. jsem obdržel(a) „Základní poučení uchazeče o zaměstnání" platné ode dne 29. 7. 2017.

L. Udělení souhlasu:

1. **Souhlasím[15] se zpracováním svých osobních údajů pro účely zprostředkování zaměstnání a pro poskytování dalších služeb podle zákona o zaměstnanosti.**
2. ☐ Souhlasím ☐ nesouhlasím, aby si krajská pobočka Úřadu práce ČR sama vyžádala údaje rozhodné pro zařazení nebo vedení v evidenci uchazečů o zaměstnání, které lze získat z úřední evidence České (okresní) správy sociálního zabezpečení.
3. ☐ Souhlasím[16] ☐ nesouhlasím, aby Úřad práce ČR předával České poště moje rodné číslo, popř. datum narození, při **všech výplatách**, které mi bude zasílat poštovní poukázkou.

Tímto žádám o zprostředkování zaměstnání, protože chci a můžu pracovat a o práci se ucházím.

V	dne . . 20	Podpis žadatele:

Totožnost žadatele byla ověřena podle dokladu:	Dne	Podpis zaměstnance:

Formuláře žádostí, potvrzení a ostatních dokladů naleznete na internetové adrese http://portal.mpsv.cz/forms nebo si je vyzvednete na pracovišti Úřadu práce ČR. Na toto pracoviště se také obraťte, pokud budete mít při vyplňování pochybnosti.

14) Uveďte název společnosti/zaměstnavatele.

15) Neposkytnutí nebo zrušení souhlasu se zpracováním osobních údajů je překážkou pro zařazení a vedení v evidenci uchazečů o zaměstnání.

16) Souhlas s předáním rodného čísla České poště je určen k zajištění výplaty peněz oprávněnému příjemci.

PŘÍLOHA P II: ŽÁDOST O PODPORU V NEZAMĚSTNANOSTI

ÚŘAD PRÁCE ČR

ZAM
PODPORA

Záznam o dni podání žádosti

OSÚ
S 15

Žádost o podporu v nezaměstnanosti

§ 39 a násl. zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů (dále jen „zákon o zaměstnanosti")

A. Žadatel:

Příjmení:	Jméno:	Rodné číslo v ČR[1]:
Rodné příjmení:	Titul před: za:	Státní příslušnost:
Místo narození[2]:		
Bydliště[3]: Obec: ..... Část obce:		
Ulice: ..... Č. p.: ..... Č. orient.: ..... PSČ:		

B. Podporu v nezaměstnanosti požaduji vyplácet:

Zaškrtněte jednu z následujících tří variant a do příslušné tabulky uveďte doplňující informace.

☐ na platební účet u peněžního ústavu v ČR vedeném v CZK:

Číslo účtu:	Kód banky:	Specifický symbol[4]:

☐ poštovním poukazem na adresu bydliště v ČR

☐ poštovním poukazem na jinou adresu v ČR:

Obec: ..... Část obce: .....
Ulice: ..... Č. p.: ..... Č. orient.: ..... PSČ: .....

C. Skutečnosti rozhodné pro přiznání a poskytování podpory v nezaměstnanosti:

1. Ke dni, k němuž má být podpora v nezaměstnanosti přiznána (den podání této žádosti nebo den zařazení do evidence uchazečů o zaměstnání)[5]:

☐ Jsem ☐ nejsem poživatelem starobního důchodu, včetně předčasného starobního důchodu.

☐ Jsem ☐ nejsem v pracovněprávním vztahu (tj. pracovní poměr, vztah na základě dohody o pracovní činnosti) nebo ve služebním poměru.

☐ Jsem ☐ nejsem

a) společníkem společnosti s ručením omezeným,
b) jednatelem společnosti s ručením omezeným,
c) komanditistou komanditní společnosti,
d) členem představenstva nebo správní rady nebo statutárním ředitelem akciové společnosti,
e) členem dozorčí rady obchodní společnosti,
f) členem družstva[6],
g) ředitelem obecně prospěšné společnosti,
h) vedoucím organizační složky zahraniční právnické osoby,
i) fyzickou osobou pověřenou obchodním vedením

vykonávajícím mimo pracovněprávní vztah k této společnosti (družstvu) pro společnost (družstvo) práci.

☐ Mám ☐ nemám nárok na výsluhový příspěvek (např. podle zákona o vojácích z povolání, zákona o služebním poměru příslušníků bezpečnostních sborů). Nárok na výsluhový příspěvek, včetně jeho výše, se dokládá rozhodnutím nebo potvrzením zaměstnavatele.

1) Cizinci, pokud nemají v ČR přiděleno rodné číslo, uvedou v kolonce **Rodné číslo v ČR** datum narození ve tvaru den, měsíc, rok a pohlaví ve tvaru: M nebo Ž (muž nebo žena).

2) Vyplňte, nebylo-li Vám přiděleno rodné číslo.

3) Za bydliště se považuje:
- u státního občana ČR adresa místa trvalého pobytu na území ČR,
- u cizince, který je občanem EU nebo jeho rodinným příslušníkem anebo rodinným příslušníkem občana ČR, adresa trvalého nebo přechodného pobytu na území ČR, a pokud takový pobyt nemá, adresa místa, kde se na území ČR obvykle zdržuje,
- u cizince, který není občanem EU ani jeho rodinným příslušníkem ani rodinným příslušníkem občana ČR, adresa místa trvalého pobytu na území ČR, je-li držitelem modré karty, adresa uvedená jako místo pobytu v agendovém informačním systému cizinců.

4) Kolonku **Specifický symbol** vyplňte pouze v případě Československé obchodní banky pro účty s číslem 6699.

5) Podpora v nezaměstnanosti náleží uchazeči o zaměstnání při splnění stanovených podmínek ode dne podání písemné žádosti o podporu v nezaměstnanosti nebo ode dne zařazení do evidence uchazečů o zaměstnání, pokud uchazeč o zaměstnání o podporu v nezaměstnanosti požádá do 3 pracovních dnů po skončení zaměstnání, jiné výdělečné činnosti nebo činnosti, která se považuje za náhradní dobu zaměstnání.

6) Uveďte pouze v případě, že nejste členem bytového družstva, který vykonává práci nebo činnost pro bytové družstvo mimo pracovněprávní vztah nebo jste pověřen obchodním vedením bytového družstva.

Tisk: Moraviapress, s.r.o. Břeclav – vzor 2017

17 08 01 804

☐ Bylo ☐ nebylo vyplaceno odstupné z posledního zaměstnání (dokládá se potvrzením zaměstnavatele).

☐ Bylo ☐ nebylo vyplaceno odbytné z posledního zaměstnání (dokládá se potvrzením zaměstnavatele).

☐ Bylo ☐ nebylo vyplaceno odchodné z posledního zaměstnání (dokládá se potvrzením zaměstnavatele).

☐ Pobírám ☐ nepobírám dávky nemocenského pojištění (nemocenské, peněžitá pomoc v mateřství, ošetřovné, vyrovnávací příspěvek v těhotenství a mateřství).

☐ Je ☐ není proti mně veden výkon rozhodnutí (exekuce). V případě nařízení výkonu rozhodnutí (exekuce) doložte usnesení soudu (exekuční příkaz) a doklad o částce dosud provedených srážek.

V době 3 pracovních dnů před podáním této žádosti jsem byl(a) v pracovní neschopnosti: ☐ ano ☐ ne

2. Dále potvrzuji:

☐ Pobíral(a) ☐ nepobíral(a) jsem v České republice podporu v nezaměstnanosti v posledních 2 letech před zařazením do evidence uchazečů o zaměstnání.

☐ Pobíral(a) ☐ nepobíral(a) jsem dávky v nezaměstnanosti ve státě EU[7] v posledních 2 letech před zařazením do evidence uchazečů o zaměstnání. Pobírání dávek se dokládá formulářem E301 nebo U1 vystaveným příslušnou institucí státu EU.

☐ Pobírám ☐ nepobírám dávky v nezaměstnanosti v jiném státě EU.

3. Poslední ukončené zaměstnání nebo jiná výdělečná činnost v posledních 2 letech před zařazením do evidence uchazečů o zaměstnání, ve které uchazeč o zaměstnání žádá o podporu v nezaměstnanosti (uveďte všechna zaměstnání a jiné výdělečné činnosti, které jste ukončil(a) ve stejný den)[7]:

Název zaměstnavatele nebo druh jiné výdělečné činnosti	Od	Do

4. Další ukončená nebo neukončená zaměstnání nebo jiné výdělečné činnosti a náhradní doby zaměstnání[8] v posledních 2 letech:

Název zaměstnavatele nebo druh jiné výdělečné činnosti nebo náhradní doby	Od	Do

☐ Souhlasím ☐ nesouhlasím, aby si krajská pobočka Úřadu práce ČR sama vyžádala údaje rozhodné pro přiznání a poskytování podpory v nezaměstnanosti, které lze získat z úřední evidence České (okresní) správy sociálního zabezpečení.

V	dne . . 20	Podpis žadatele:

Totožnost žadatele byla ověřena podle dokladu:	Dne	Podpis zaměstnance:

Formuláře žádostí, potvrzení a ostatních dokladů naleznete na internetové adrese http://portal.mpsv.cz/forms nebo si je vyzvednete na pracovišti Úřadu práce ČR. Na toto pracoviště se také obraťte, pokud budete mít při vyplňování pochybnosti.

7) **Údaje o zaměstnání a další rozhodné skutečnosti pro přiznání a poskytování podpory v nezaměstnanosti je uchazeč o zaměstnání povinen doložit**, a to například evidenčním listem důchodového pojištění, potvrzením o zaměstnání, potvrzením zaměstnavatele o výši průměrného měsíčního čistého výdělku a dalších skutečnostech rozhodných pro posouzení nároku na podporu v nezaměstnanosti, dokladem o výkonu jiné výdělečné činnosti, u osoby samostatně výdělečně činné potvrzením o získané době důchodového pojištění a o posledním vyměřovacím základu, v případě zaměstnání v členském státě Evropské unie nebo Evropského hospodářského prostoru (Island, Lichtenštejnsko, Norsko) nebo ve Švýcarsku (dále jen „EU") formulářem E301 nebo U1.

8) **Za náhradní dobu zaměstnání se považuje doba** přípravy osoby se zdravotním postižením k práci, doba pobírání plného invalidního důchodu pro invaliditu třetího stupně, doba osobní péče o dítě ve věku do 4 let a doba osobní péče o fyzickou osobu mladší 10 let, která se podle zákona o sociálních službách považuje za osobu závislou na pomoci jiné fyzické osoby ve stupni I (lehká závislost). Dále doba osobní péče o fyzickou osobu, která se podle zákona o sociálních službách považuje za osobu závislou na pomoci jiné fyzické osoby ve stupni II (středně těžká závislost), ve stupni III (těžká závislost) nebo ve stupni IV (úplná závislost), pokud s uchazečem o zaměstnání trvale žije a společně uhrazují náklady na své potřeby; tyto podmínky se nevyžadují, jde-li o osobu, která se pro účely důchodového pojištění považuje za osobu blízkou. Za náhradní dobu se rovněž považuje doba výkonu dlouhodobé dobrovolnické služby na základě smlouvy dobrovolníka s vysílající organizací, která byla udělena akreditace Ministerstvem vnitra, nebo výkonu veřejné služby na základě smlouvy o výkonu veřejné služby, pokud rozsah vykonané služby překračuje v průměru alespoň 20 hodin v kalendářním týdnu a dále doba trvání dočasné pracovní neschopnosti nebo nařízené karantény osoby po skončení výdělečné činnosti, která zakládala její účast na nemocenském pojištění podle zákona o nemocenském pojištění, pokud si tato osoba nepřivodila dočasnou pracovní neschopnost úmyslně a pokud tato dočasná pracovní neschopnost nebo nařízená karanténa vznikla v době této výdělečné činnosti nebo v ochranné lhůtě podle zákona o nemocenském pojištění.

Platnost tiskopisu od 29.7.2017. 17 08 01 804

ŘÍLOHA P III: OZNÁMENÍ ZMĚNY ADRESY

Oznámení změny adresy

□ trvalého bydliště:

.....

□ doručovací adresy:

.....

Datum:

jméno příjmení (hůlkovým písmem):

podpis:

ŘÍLOHA P IV: OZNÁMENÍ O ZMĚNĚ ZPŮSOBU VÝPLÁCENÍ PODPORY V NEZAMĚSTNANOSTI

Oznámení o změně způsobu vyplácení podpory v nezaměstnanosti

□ na číslo účtu:

……

□ poštovní poukázkou na adresu:

……

……

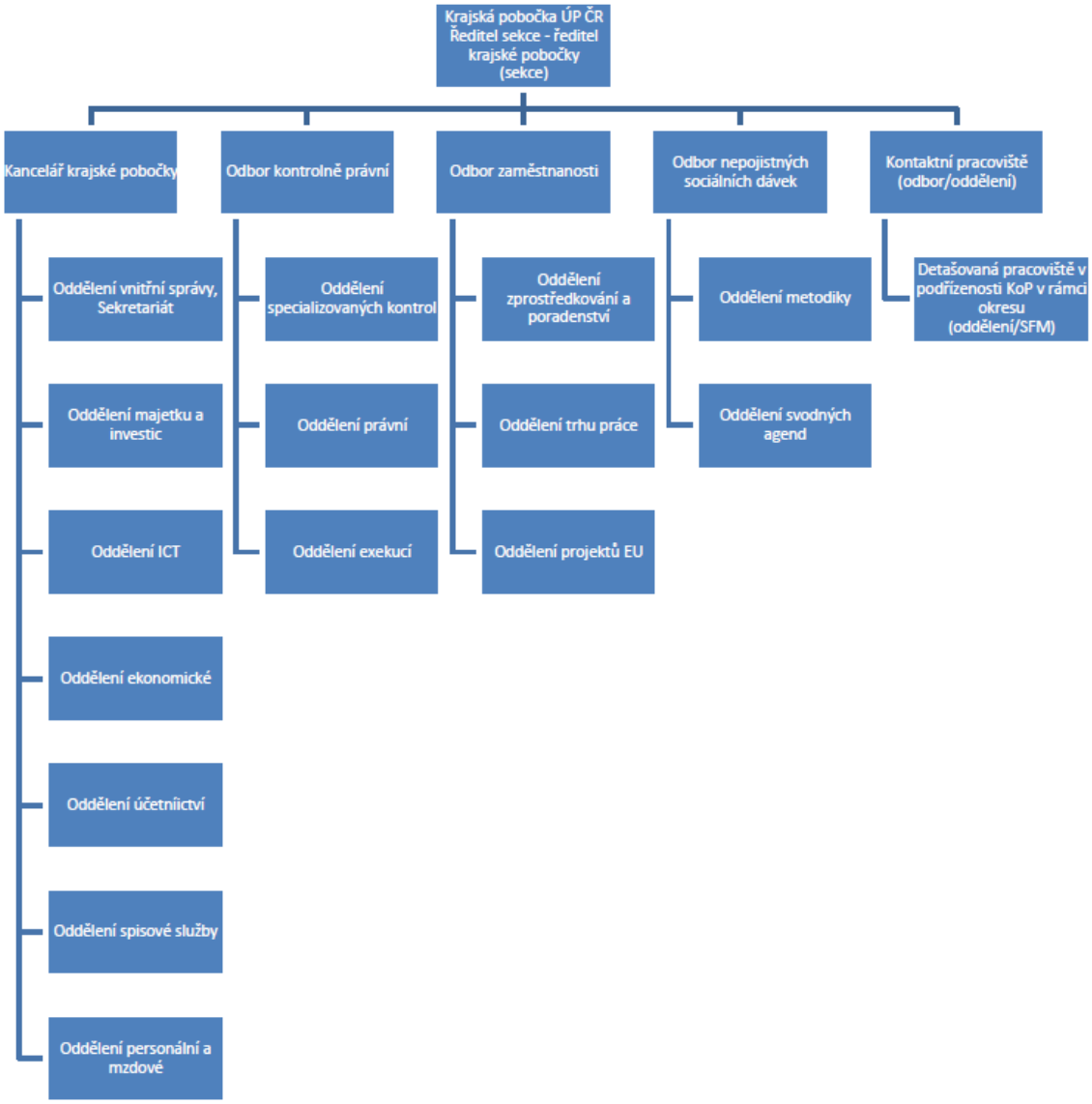
……

datum:

jméno příjmení (hůlkovým písmem):

podpis:

ŘÍLOHA P V: ORGANIZAČNÍ STRUKTURA KRAJSKÝCH POBOČEK



ŘÍLOHA P VI: STÁVAJÍCÍ DISLOKACE PRACOVIŠŤ ÚP NA ÚZEMÍ JIHOMORAVSKÉHO KRAJE