Aplikace zákona 101/2000 Sb., při ochraně osobních údajů zpracovávaných ve mzdových agendách

Application of Act 101/2000 with Protection of Personal Data within Salary Administration

Jana Macalová

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

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

Jméno a příjmení:	**Jana MACALOVÁ**
Osobní číslo:	**A08866**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Aplikace zákona 101/2000 Sb., při ochraně osobních údajů zpracovávaných ve mzdových agendách**

Zásady pro vypracování:

1. **Seznamte bezpečnostní komunitu s problémy ochrany osobních údajů v podmínkách státní správy.**
2. **Popište problém ve vztahu k zákonu č.101/2000 Sb.**
3. **Uveďte formy zabezpečení ochrany osobních údajů a dat.**
4. **Stanovte možné problémy vyplývající z problematiky zabezpečení ochrany osobních údajů a dat a popište možná řešení problémů.**
5. **Specifikujte sankce vyplývající ze zákona 101/2000 Sb. ve vztahu k problematice.**
6. **Proveďte seznámení se s předpokládaným vývojem v problematice.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Zákon 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů ze dne 4. dubna 2000, zákon vyhlášen 25. 4. 2000 ve Sbírce zákonů v částce 32 pod číslem 101/2000 Sb.**
2. **Kolektiv autorů. Autentizace uživatelů a autorizace elektronických transakcí, příručka manažera. Vydáno TATE International, s.r.o., v Praze v listopadu 2007 ISBN 978-80-86813-14-1.**
3. **JUDr. Vladimír Lacký. Řízení technologických procesů v průmyslu komerční bezpečnosti. Vydáno Univerzitou Tomáše Bati ve Zlíně v červnu 2006 ISBN 80-7318-432-X.**
4. **JUDr. Vladimír Lacký. Technologie komerční bezpečnosti I. Vydáno Univerzitou Tomáše Bati ve Zlíně v roce 2010 ISBN 978-80-7318-889-4.**
5. **JUDr. Vladimír Lacký. Technologie komerční bezpečnosti II. Vydáno Univerzitou Tomáše Bati ve Zlíně v roce 2007 ISBN 978-80-7318-631-9.**

Vedoucí bakalářské práce: **JUDr. Vladimír Lacký**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Bakalářská práce si klade za cíl popsat způsob, jakým je zajišťována ochrana osobních údajů v Ekonomickém informačním systému Ministerstva vnitra. V bakalářské práci je popsána aplikace zákona 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a aplikace směrnic MV ve vztahu k architektuře informačního systému, autorizaci i autentizaci uživatelů informačního systému. Pomocí materiálů poskytnutých pracovištěm bezpečnostního manažera Ekonomického informačního systému bylo provedeno vyhodnocení bezpečnosti Ekonomického informačního systému. V příloze bakalářské práce seznamuji s formuláři, které jsou nutné k udělení oprávnění vstupu do Ekonomického informačního systému EKIS.

Klíčová slova:

Ochrana osobních údajů, autentizace uživatelů, autorizace uživatelů, Ekonomický informační systém MV (EKIS), bezpečnostní požadavky, bezpečnostní manažer, oprávněný uživatel, architektura bezpečnosti systému, personální bezpečnost

ABSTRACT

The Bachelor Thesis proposes to describe the way personnel information security in the Economic Information System of Ministry of Interior is ensured.

The Bachelor Thesis describes application of law 101/2000 Sb., about personnel information security, and about amendment of acts, and application of directives of Ministry of Interior in relation to architecture of information system, authorization and the information system users authentication.

Security evaluation of the Economic Information System was realized with help of materials provided by department of Security manager of the Economic Information System.

In the Annex are introduced the forms necessary for grant of authorization of permission into the Economic Information System EKIS.

Keywords:

Personnel information security, users authentication, users authorization, Economic Information System of Ministry of Interior EKIS, safety requirements, security manager, authorized user, architecture of information system, personnel security

Poděkování, motto

Děkuji panu JUDr. Vladimíru Lauckému a panu JUDr. Jiřímu Kameníkovi za vedení mé práce a cenné rady a podnětné připomínky při tvorbě této práce. Děkuji panu Ing. Jiřímu Minichbauerovi za poskytnuté materiály a rady, které jsem využila při tvorbě této práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním 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 bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk 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 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 – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Ve své práci se zaměřuji na výklad pojmu ochrana osobních údajů v prostředí Ekonomického informačního systému Ministerstva vnitra ČR, kde se zaměřuji především na mzdovou agendu.

Ekonomický informační systém Ministerstva vnitra ČR je určen pro zpracování finančního účetnictví, materiálních evidencí, mezd a služebních příjmů zaměstnanců ministerstva vnitra, personálních agend a vzdělávání. Systém je v pronájmu na základě nájemní smlouvy mezi IBM Česká republika, s.r.o. a Ministerstvem vnitra České republiky.

V práci jsou uvedeny principy zabezpečení dat v tomto systému. Podrobně jsou zde zpracovány principy přístupu oprávněných uživatelů k osobním údajům.

I. TEORETICKÁ ČÁST

1 DEFINOVÁNÍ POJMU OSOBNÍ ÚDAJ

Pojem „osobní údaj“ je definován v právních předpisech

§ 4 písm. a) zákona 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů: „Osobním údajem se rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“

Kde dle § 4 písm. b) zákona 101/2000 Sb.:

„Citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů, citlivým údajem je také biometrický údaj, který umožňuje přímou nebo identifikaci nebo autentizaci subjektu údajů.“

a dle § 4 písm. d) zákona 101/2000 Sb.:

„Subjektem údajů fyzická osoba, k níž se osobní údaje vztahují.“

Čl. 2 odst. a) Směrnice evropského parlamentu a rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů: „Osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů), identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity.“

Čl. 2 odst. a) Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat (publikováno v Sdělení č. 115/2001 Sb.m.s. Ministerstva zahraničních věcí ČR): „Osobní údaje znamenají každou informaci týkající se identifikované nebo identifikovatelné fyzické osoby („subjekt údajů“).

Osobní údaje jsou informace, které se vztahují ke konkrétní osobě. Údaje, podle kterých jsme schopni konkrétní fyzickou osobu identifikovat (např. rodné číslo, jméno a příjmení), ale i údaje, které se vztahují ke konkrétní osobě (oblíbené jídlo, barva očí….).

Osobní údaj se vztahuje výhradně k fyzické osobě, nikoli k osobě právnické.

1.1 Nejvýznamnější zdroje osobních údajů

Subjekt údajů

Veřejné zdroje

Jiný správce osobních údajů

Správce samotný

2 TYPOLOGIE OSOBNÍCH ÚDAJŮ

Aspekty lidské existence, o kterých osobní údaje vypovídají			**Osobní údaje**	**Rozdělení osobních údajů na citlivé a ostatní**
Člověk jako biologická bytost	Údaje související s narozením		Rok narození	
			Datum narození	
			Místo narození	
			Pohlaví	
	Sexualita		Sexuální život	citlivé
	Původ		Rasový původ	citlivé
			Genetické údaje	citlivé
	Zdravotní stav		Nemoci	citlivé
			Úrazy	citlivé
	Biometické údaje	Fyzikální hodnoty vztahující se k člověku	Velikost oblečení	citlivé
			Velikost bot	citlivé
			Výška postavy	citlivé
			Váha osoby	citlivé
			Otisky prstů	citlivé
			Barva očí	citlivé
			Záznam hlasu	citlivé
		Podobizny - vizuální pozorování člověka	Fotografie	citlivé
			Tetování	citlivé
			Piersing	citlivé
			Posmrtné masky (pokud jsou udělány živému člověku	citlivé
		Chemicko fyzikální hodnoty vztahující se k člověku	DNA	citlivé
			Rentgenové snímky	citlivé
			Krevní skupina	citlivé
			EKG	citlivé
			EEG	citlivé
			Oční pozadí	citlivé
Člověk jako sociální bytost	Pojmenování osoby		Jméno	
			Přijmení	
	Usídlení osoby		Trvalý pobyt	
			Přechodné bydliště	
	Vztah k osobám z hlediska původu	Příbuzenské vztahy	Děti	
			Rodiče	
			Manžel	

Aspekty lidské existence, o kterých osobní údaje vypovídají			**Osobní údaje**	**Rozdělení osobních údajů na citlivé a ostatní**
Člověk jako sociální bytost	Vztah k osobám z hlediska původu	Příbuzenské vztahy	Sourozenci	
			Ostatní příbuzní	
		Mimopříbuzenské vztahy	Národnostní původ	citlivé
			Etnický původ	citlivé
	Vztah ke státu	Státní příslušnost	Státní příslušnost	
		Identifikace subjektu pro výkon funkcí státu	Rodné číslo	
			Číslo občanského průkazu	
			Číslo pasu	
		Plnění branné povinnosti	Voják/nevoják	
			Vojenská hodnost	
		Stav	ženatý/vdaná	
		Zdravotní pojišťovna	Odvádění pojistného	
		Sociální dávky	Poskytované soc. dávky	
		Spáchání přestupku	Spáchání přestupku	
		Spáchání trestného činu	Spáchání trestného činu	citlivé
		Výkon veřejné funkce	Výkon veřejné funkce	
		Omezení způsobilosti k právním úkonům	Omezení způsobilosti k právním úkonům	
		Udělená vyznamenání	Udělená vyznamenání	
		Spolupráce s STB	Faktická spolupráce s STB	
			Vedení v seznamech STB	
			Lustrační osvědčení	
		Držba oprávnění k provozování určité činnosti	Řidičské oprávnění	
			Živnostenské oprávnění	
			Jiné podnikatelské oprávnění	
			Ostatní oprávnění (lovecký lístek, rabářský lístek)	
			Oprávnění seznamovat se s utajovanými skutečnostmi	
			Zbrojní průkaz, evropský zbrojní pas	

Aspekty lidské existence, o kterých osobní údaje vypovídají			**Osobní údaje**	**Rozdělení osobních údajů na citlivé a ostatní**
Člověk jako sociální bytost	Vztah k jiným subjektům práva	v rámci soužití	Manželé	
			Druhové	
		Obchodní partneři	Obchodní partneři	
		Spotřebitelé	Spotřebitelé	
		Zaměstnavatelé	Zaměstnavatelé	
		Pojišťovny	Druhy pojištění	
		Banky	Číslo účtu	
			Úvěry	
	Majetkové poměry (vlastnictví věcí a práv)	Věcná břemena	Věcná břemena	
		Movité věci	Auta	
			Lodě	
			Letadla	
			Zbraně	
			Cenné papíry	
			Telefonní číslo	
		Průmyslová práva	Průmyslová práva	
		Autorská práva	Autorská práva	
		Práva příbuzná právu autorskému	Práva příbuzná právu autorskému	
		Ostatní nehmotný majetek	Emailová adresa	
			Doménová jména	
			Know how	
		Živá zvířata	Živá zvířata	

Aspekty lidské existence, o kterých osobní údaje vypovídají			**Osobní údaje**	**Rozdělení osobních údajů na citlivé a ostatní**
Člověk jako sociální bytost	Myšlení a přesvědčení	Vzdělání	Dosažené vzdělání	
			Začátek a ukončení studia	
			Studijní prospěch	
			Absolvované zkoušky	
			Studijní úspěchy	
			Akademický titul	
			Vědecká hodnost	
		Politické postoje	Členství v politické straně	citlivé
			Politické názory	citlivé
		Filozofické přesvědčení	Členství v odborech	citlivé
			Filozofické názory	citlivé
			Vyznávané náboženství	citlivé
	Koníčky	Sport	Dosažené soutěžní úspěchy	
			Dosažené sportovní výsledky	
			Registrace ve sportovních sdruženích	
		Hobby	Dosažené soutěžní úspěchy	
			Dosažené výsledky	
			Registrace v zájmových sdruženích	

tabulka č. 1 : Typologie osobních údajů

II. PRAKTICKÁ ČÁST

4 PROBLÉMY OCHRANY OSOBNÍCH ÚDAJŮ V PODMÍNKÁCH STÁTNÍ SPRÁVY

Řešení otázky ochrany osobních údajů bude specifikováno na podmínky Ministerstva vnitra ČR, konkrétně na oblast EKONOMICKÉHO INFORMAČNÍHO SYSTÉMU MV ČR (EKIS).

V devadesátých letech minulého století byl do podmínek MV ČR implementován informační systém EKIS I, který je určen pro vedení účetnictví a materiálových evidencí. Na tento systém se navázalo implementováním části EKIS II. Tato část je zaměřena na zpracování mezd, personální agendy a vzdělávání. K ostrému provozu této části došlo v roce 2004. Právě informačním systémem EKIS II ve vztahu k problematice osobních údajů se bude tato práce zabývat.

V rámci rezortu ministerstva vnitra EKIS II využívají tyto organizační jednotky:

Úřad ministerstva vnitra (vlastní ministerstvo)

Policejní prezídium ČR

Policie ČR (krajská ředitelství, útvary s celorepublikovou působností)

Generální ředitelství hasičského záchranného sboru

HZS Hlučín

Školy (včetně Policejní akademie ČR)

Státní oblastní archívy

Muzeum Police ČR

Centrum sportu MV ČR

Správa uprchlických zařízení MV ČR

Systém tvoří moduly

PA – personální administrace : umožňuje zpracování potřebných údajů o zaměstnancích rezortu (personalistika, mzdy a sociální evidence)

PD – personální vývoj: umožňuje práci s organizační strukturou MV (systemizace – údržba a plánování systemizovaných míst a vzdělávání plánování vzdělávání pracovníků)

WEB – jedná se o nadstavbu systému, která umožňuje vedoucím pracovníkům (do úrovně vedoucí oddělení), nebo jimi pověřeným pracovníkům (plánovači služeb) prostřednictvím webového rozhraní přístup do systému EKIS II WEB umožňuje zasílání plánů služeb (směn), nepřítomností, osobních změn přímo do kmenových dat zaměstnanců. Současně vedoucím pracovníkům v omezené míře umožňuje čerpat informace ze systému EKIS.

EKIS je vybudován jako centrální systém, jehož základ tvoří softwarový produkt Systém R/3 od firmy SAP a jako podpůrný systém je WEB aplikace LOTUS DOMINO. Hardware i software je pronajatý od firmy IBM Česká republika, spol. s r.o. a je umístěný ve výpočetním středisku MV. Odpovědnost za funkčnost centrální části má pronajímatel (IBM), který je zároveň garantem správného nastavení systému podle podkladů dodaným ministerstvem vnitra. Ministerstvo vnitra v plném rozsahu zabezpečuje přístup k systému prostřednictvím sítí WAN a LAN a zodpovídá za funkčnost a bezpečnost těchto sítí. Všechna pracoviště využívající informační systém EKIS mají přístup do systému zabezpečen těmito sítěmi.

Bezpečnostní požadavky na EKIS

Bezpečnostní požadavky na systém EKIS jsou obsaženy ve smlouvě mezi IBM s.r.o. a ministerstvem vnitra. Dále jsou specifikovány v cílovém konceptu, dle něhož byl systém implementován.

Bezpečnost informačního systému tvoří systém opatření z oblasti fyzické, personální, režimové, technické, programové, datové a komunikační bezpečnosti. Tato bezpečnost je definována v bezpečnostní dokumentaci informačního systému. V systému EKIS II se nepředpokládá zpracování informací podléhající klasifikaci podle zákona č. 413/2005 ve znění pozdějších předpisů.

V systému EKIS se zpracovávají osobní data policistů a pracovníků MV ČR, proto vycházejí bezpečnostní požadavky na systém z právních norem upravující zpracování těchto údajů:

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

Nařízení Ministerstva vnitra č. 48 ze dne 18. srpna 2006, kterým se upravuje postup při ochraně osobních údajů v Ministerstvu vnitra a Policii České republiky

Nařízení Ministerstva vnitra č. 52 ze dne 13. září 2006, o personální evidenci a o zpracování osobních údajů, které s ní souvisejí

Provozní řád Ekonomického informačního systému Ministerstva vnitra ČR

Zakoupené právo využívání českého překladu normy ISO IEC 1799:2000 a BS 7799-2:2002

Přístup k informacím v systému musí být řízený. Osobní údaje je možné zpřístupnit pouze určeným osobám. Přidělení přístupového oprávnění do informačního systému se řídí schváleným přístupem (Provozní řád EKIS). Bez jeho dodržení nelze z bezpečnostních důvodů přístup do EKIS zřídit.

Fyzická bezpečnost

Ochrana všech zařízení centrálního systému před volným přístupem nepovolaných osob. Evidence všech osob, kterým byl umožněn přístup k technickým zařízením centrální části systému. Ochrana pracovních stanic proti neoprávněnému přístupu a neodborné manipulaci s nimi.

Personální bezpečnost

Kvalifikovaný výběr budoucích uživatelů, řádné vyškolení uživatelů ve všech činnostech, které budou v informačním systému provádět, proškolení uživatelů v bezpečnosti informačního systému a seznámení uživatelů s povinnostmi vyplývajícími z uvedených právních norem.

Režimová bezpečnost

Zajištění dodržování všech právních norem, kterými se EKIS řídí. Provádění kontroly v dodržování bezpečnosti EKIS. Zkoumání záznamů z prováděných auditů v IS v termínech stanovených bezpečnostní dokumentací IS.

Technická bezpečnost

Řešení ochrany dat použitím odpovídajících technických prostředků, zajištění potřebné spolehlivosti a servisních služeb.

Zálohování databáze takovým způsobem, aby byla umožněna jejich obnova v určeném časovém okamžiku.

Programová a datová bezpečnost

Zajištění jednoznačné identifikace a autentizace uživatele, která musí předcházet všem dalším aktivitám uživatelů v informačním systému. Zajištění ochrany důvěrnosti a integrity autentizací informace.

Volitelné řízení přístupu k objektům na základě definice přístupových práv uživatele a identity uživatele nebo jeho členství ve skupině uživatelů.

Nepřetržité monitorování událostí, které mohou ovlivnit bezpečnost informačního systému, zaznam do auditních záznamů.

Zabezpečit auditní záznamy před neautorizovaným přístupem, modifikací, zničení.

Záznam chybných přihlášení, pokusů o zkoumání přístupových práv, vytváření nebo rušení objektu a nebo činnost autorizovaných uživatelů, která by ovlivňovala bezpečnost informačního systému.

Datová bezpečnost

Požadavek na zálohování. Vzhledem k charakteru a množství zpracovávaných informací chránit databázi před neoprávněnými změnami, poškozením nebo ztrátou.

5 DOSTUPNOST INFORMAČNÍHO SYSTÉMU V ČASE

Vzhledem k tomu, že informace zpracovávané v informačním systému jsou důležité k činnosti policistů i pracovníků, je jejich zpřístupnění požadováno a realizováno následujícím způsobem.

Zpřístupnění pro zadávání nových nebo aktualizace již existujících dat:

pondělí až pátek 6:30 – 18:00 hodin

Zpřístupnění pro vytěžování vybraných informací nepřetržitě po celý týden 24 hodin denně.

Uživatelům je umožněno požádat o administraci a přístup do systému i v mimopracovní době. V případě mzdových agend je to například období, kdy se zpracovává daň z příjmů, agendy spojené s ukončením období apod. V tomto případě zašlou žádost (specifikováno v provozním řádu EKIS) na kompetenční centrum EKIS.

6 VYMEZENÍ ODPOVĚDNOSTI VE VZTAHU K EKIS

Vlastník EKIS:

Vrcholový manažer odpovědný za EKIS jako celek ministru vnitra. Dle provozního řádu EKIS se jedná o náměstka ministra vnitra odpovědného za ekonomiku. Vlastník deleguje svoji pravomoc ve vztahu k řízení procesů EKIS zodpovědné osobě do role ředitele realizace EKIS, kterého jmenuje dekretem. Organizačním řádem MV jsou určeny útvary odpovědné za vztah k datům v systému tzv. vlastníka dat. Organizačním řádem je dále stanoven útvar zajišťující bezpečnost EKIS. Vlastník EKIS jmenuje dekretem odpovědnou osobu do role bezpečnostního manažera a deleguje jí veškeré pravomoci v oblasti bezpečnosti EKIS. Ve vztahu k plánování rozvoje a financování EKIS je organizačním řádem stanoven Projektant a Investor EKIS.

Ředitel realizace EKIS

Zodpovědná osoba pověřená vlastníkem řízením realizace příslušné etapy EKIS. Ředitel EKIS dává ředitelům s dispozičním oprávněním II. a III. stupně podnět ke jmenování a odvolávání odpovědných osob EKIS na organizačních jednotkách. Schvaloval žádosti o zařazení uživatelů a administrátorů do EKIS ve fázi náběhu. Ředitel EKIS má delegované pravomoci a zodpovědnost potřebné pro příslušná ohodnocení a rozhodnutí, týkající se používání, identifikace a klasifikace EKIS jako celku nebo určité části.

Vlastník dat

Útvar MV (PČR) určený organizačním řádem zodpovědný za kontrolu a vytěžování dat EKIS. Zodpovídá za klasifikaci dat a metodické řízení uživatelů, kteří data pořizují.

Pro účely přístupových oprávnění se rozlišují pojmy

Primární vlastník dat – vedoucí pracovník organizačního celku s personální pravomocí

Sekundární vlastník dat – ředitel personálního odboru MV ČR

Investor EKIS

Útvar MV určený organizačním řádem zodpovědný za správu finančních prostředků použitých na realizaci, rozvoj a provoz EKIS. Investor EKIS zodpovídá za hospodárné vynakládání rozpočtových výdajů určených pro projekt EKIS.

Projektant EKIS

Útvar MV určený organizačním řádem zodpovědný za přípravu, rozvoj a údržbu EKIS. Projektant EKIS má v pracovní náplni upravené pravomoci a zodpovědnost potřebné pro příslušná ohodnocení a rozhodnutí, týkající se přípravy, rozvoje a údržby EKIS jako celku nebo jeho části.

Bezpečnostní manažer EKIS

Zodpovědná osoba pověřená vlastníkem řízením bezpečnosti EKIS. Bezpečnostní manažer dává ředitelům s dispozičním oprávnění II. a III. stupně podnět ke jmenování a odvoláním bezpečnostního správce pro příslušný účetní okruh. Dále schvaluje protokol o zařazení uživatele a administrátorů do EKIS. Bezpečnostní manažer EKIS má v pracovní náplni upravené pravomoci a zodpovědnost potřebné pro příslušná ohodnocení a rozhodnutí, týkající se ochrany EKIS jako celku nebo určitého aktiva.

Správce EKIS

Výkon správce EKIS zajišťuje v souladu s organizačním řádem MV provoz EKIS a je odpovědný za správnou administraci systému. Správce systému dává ředitelům s dispozičním oprávněním II. a III. stupně podnět ke jmenování a odvolávání administrátorů koncových stanic. Vedoucí provozu centrální části EKIS má v pracovní náplni upravené pravomoci a zodpovědnost pro příslušná rozhodnutí, týkající se používání, správy EKIS jako celku nebo určité části.

Manažer nastavení EKIS

Manažer nastavení EKIS je určen ředitelem realizace EKIS a je osobně spoluodpovědný za správné nastavení příslušných modulů systému, zejména po metodické stránce. Manažer nastavení EKIS má v pracovní náplni upravené pravomoci a zodpovědnost pro příslušná rozhodnutí, týkající se metodiky EKIS jako celku nebo určité části. Předkládá požadavky příslušným útvarům na vypracování příslušných metodických předpisů.

Správce číselníků EKIS

Výkon správce číselníků EKIS zajišťuje útvar stanovený organizačním řádem a je odpovědný za správné nastavení a tvorbu jednotlivých uživatelských číselníků. Má ve své pracovní náplni upravené pravomoci a zodpovědnost potřebné pro příslušná rozhodnutí, týkající se metodiky tvorby číselníků EKIS jako celku nebo určité části předkládá požadavky příslušným útvarům na vypracování příslušných metodických předpisů ve vztahu k číselníkům EKIS.

Odpovědná osoba

Je jmenována vedoucím pracovníkem organizační jednotky. Má pravomoc a zodpovědnost na úseku organizační jednotky za dodržování všech organizačních aktivit na svěřeném úseku. Tuto roli je u menších útvarů možné kumulovat s bezpečnostním správcem.

Administrátor

Administrátor koncových stanic – odpovídá na dané organizační jednotce za administraci koncových stanic. Je jmenován a odvolán vedoucím pracovníkem se personální pravomocí.

Administrátor centrální části – je odpovědný za administraci Centrální části EKIS

Z hlediska bezpečnosti informačního systému jsou stěžejní tyto povinnosti administrátora centrální části:

Všechny kroky prováděné při administraci a obsluze operačního systému mající vztah k bezpečnosti EKIS a všechna závažná zjištění musí být zaznamenávány s datem, časem a popisem, kroku, postupu a výsledku do provozního deníku serverů.

Administrátor v rámci obsluhy centrální části je povinen pravidelně archivovat bezpečně ukládat, monitorovat a vyhodnocovat tyto záznamy:

chybový log AIX

bezpečnostní auditní záznamy AIX

bezpečnostní auditní záznam TCP/IP

záznam o činnosti záložního systému ADSM, vždy po ukončení automatického cyklu zálohování a vždy po ukončení ručně aktivovaného zálohování. O provedení kontroly a jejího výsledku je třeba provést záznam v povozním deníku. Pro zálohování je nutno používat zásadně pouze předem označené a evidované páskové kazety. Kazety s nově vytvořenou zálohou je nutno bezpečně uložit (uzamčený trezor s vysokou odolností proti požáru umístěný v jiné lokalitě)

Pokud administrátor zjistí z kontroly uvedených záznamů skutečnost, která nějakým způsobem ohrožuje bezpečnost provozu EKIS nebo muže být potencionální hrozbou neprodleně o tom uvědomí bezpečnostního manažera EKIS.

Oprávněný uživatel

Pořizují a editují data. Uživatele jsou dále podrobněji členěni podle uživatelských rolí a systému jsou zařazováni v souladu s pravidly stanovenými Provozním řádem.

Z hlediska bezpečnosti je velmi důležitá funkce **bezpečnostního správce**, proto je tato činnost rozepsána podrobněji:

Bezpečnostní správce EKIS je jmenován a odvoláván vedoucím pracovníkem na podnět bezpečnostního manažera. Má vymezenou pravomoc a zodpovědnost na organizační jednotce za dodržování bezpečnostních pravidel, služeb a mechanizmů na svěřeném úseku. Pokud by zejména u menších útvarů došlo ke kumulaci této role s rolí administrátora koncové stanice, je třeba častěji a velmi důkladně provádět všechny kontrolní činnosti předepsané v Provozním řádu EKIS

Činnosti a odpovědnost bezpečnostního správce:

Podílí se na zajištění bezpečnosti EKIS a na kontrole bezpečnostních funkcí na úrovni koncového uživatele.

Vyhodnocuje nahlášené bezpečnostní incidenty z hlediska potencionálního a skutečného ohrožení EKIS, provádí návrh způsobu řešení, předává informace o bezpečnostních incidentech vlastníkovi EKIS.

Provádí pravidelná, směrnicí pro činnost bezpečnostních správců stanovaná, podrobná vyhodnocení všech systémových a bezpečnostních záznamů (logů). Předává zprávu

bezpečnostnímu manažerovi EKIS. O každé kontrole musí být proveden zápis v provozním deníku a v provozním deníku bezpečnostního správce.

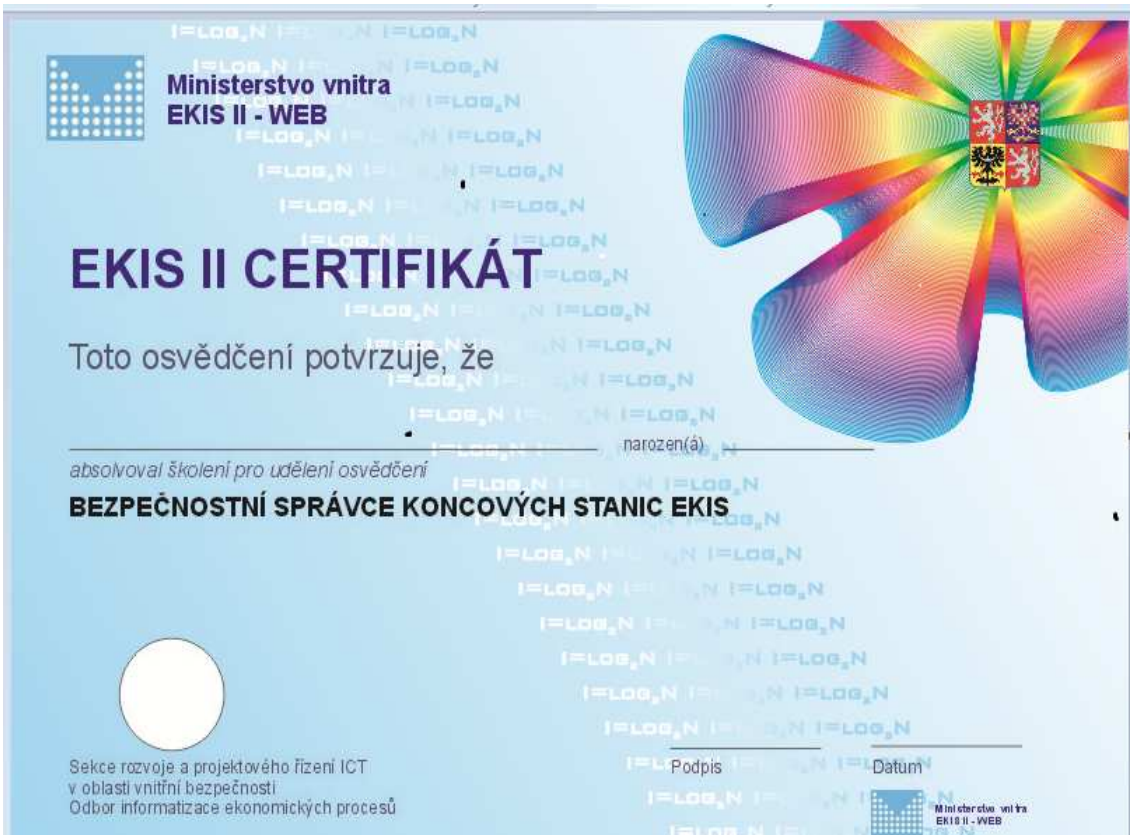
Pravidelně kontroluje dodržování bezpečnostních pravidel administrátory a uživateli EKIS

Kontroluje nastavení a účinnost bezpečnostních funkcí pracovních stanic.

Provádí pravidelné testování účinnosti plánu obnovy činnosti EKIS a návrh úprav a potřebných preventivních opatření.

Porovnává ve stanovených intervalech adresní knihu s databází vlastníkem schválených uživatelů. Kontrola, zda nebyl vytvořen neoprávněný uživatel.

Jak již bylo řečeno bezpečnostní správce je jmenován vedoucím pracovníkem na podnět bezpečnostního manažera. Bezpečnostní manažer před doporučením provede proškolení a poučení potencionálního bezpečnostního správce. K oprávnění výkonu této funkce obdrží certifikát.



Obrázek č. 1 Certifikát bezpečnostního správce EKIS

Popis výše uvedených rolí je uváděn pro vytvoření celkového přehledu o struktuře Ekonomického informačního systému EKIS. Osoby, které role vykonávají, mohou, ale nemusí být oprávněným uživatelem EKIS. Tyto osoby nemusí mít oprávnění k přístupu do systému EKIS, nemusí mít možnost vytěžovat data ze systému EKIS. Kromě samotné role oprávněného uživatele EKIS, ten samozřejmě uživatelem je. Způsob umožnění přístupu do systému EKIS a jednotlivé druhy uživatelů bude řešen v následujících částích.

7 POŽADAVKY PRONAJÍMATELE (IBM ČR, S.R.O) NA BEZPEČNOSTNÍ ASPEKTY SYSTÉMU EKIS

V uzavřené smlouvě mezi IBM, s.r.o. byly a MV ČR byly pronajímatelem jasně stanoveny základní požadavky na nájemce (MV ČR). Tyto požadavky jsou uplatňovány i v dodatcích ke smlouvě, kterými se pronájem ekonomického informačního systému prodlužuje.

7.1 Požadavek na komunikační infrastrukturu (výpis čl. 13 smlouvy o pronájmu systému)

Komunikační infrastruktura a síťové služby jsou poskytovány nájemcem a pronajimatel za jejich dostupnost ani kvalitu nenese odpovědnost.

Nájemce se zavazuje, že nejpozději dva týdny před dodávkou zařízení určí v rámci řešených úloh informace potřebné pro konfiguraci systémových zdrojů a programového vybavení centra EKIS i koncových stanic EKIS, které budou konfigurovány v rámci implementace systému.

Nájemce umožní v případě potřeby a po vzájemné dohodě pronajímateli implementovat v síti poskytnuté nájemcem pro systém programové vybavení, které bude sloužit k ověření funkčnosti služeb sítě, nutné k provozu systému.

Nájemce se zavazuje, že v termínech stanovených řídící radou poskytne řešiteli datovou síť s funkční implementací protokolové sady TCP/IP pro účely komunikace mezi servery a klienty systému. Datová síť bude splňovat přenosové parametry uvedené v příloze smlouvy (viz výpis z přílohy). Nájemce se zavazuje, že budou v poskytnuté datové síti nad protokolovou sadou TCP/IP implementovány síťové služby uvedené v příloze smlouvy (viz výpis z přílohy).

Nájemce se zavazuje splnit požadavky uvedené v odstavcích 1-5 čl. 13 v rámci všech lokalit, kde požaduje nasazení systému.

Pokud v průběhu projekčních prací, implementačních prací nebo provozu bude nájemce požadovat změnu lokality nasazení systému, je povinen tuto změnu písemně sdělit řediteli projektu pronajímatele minimálně 3 týdny před jejich uskutečněním.

Nájemce zajistí konektivitu na fyzické úrovni s rozhraním 10BaseT, 10Base2 nebo s rozhraním dia-up pro všechny klientské stanice systému. Tato konektivita bude dostupná nejméně 3 dny před termínem instalalace technického vybavení systému v lokalitě. Technický způsob připojení do sítě poskytnuté nájemce pro systém bude dohodnut realizačním týmem, a to nejméně 4 týdny před termínem instalace technického vybavení systému v lokalitě.

Pronajímatel během výstavby a provozu systému nenaruší provoz datové sítě nájemce ani provoz jiných informačních systémů nad touto síti provazovaných.

Pronajímatel bude během implementace systému postupovat v souladu s bezpečnostními požadavky nájemce, o kterých bude nájemcem písemně informován. Pokud by dodržování těchto bezpečnostních předpisů mělo vliv na časový harmonogram či použití dodatečných zdrojů pronajímatelem, bude takováto okolnost předmětem změnového řízení popsaného v článku 9 této smlouvy.

Pokud bude veškerý hardware centrální části systému umístěn v jediné lokalitě, pronajímatel zajistí jejich síťové propojení v kvalitě a funkci požadované systémem.

7.2 Výpis z přílohy ke smlouvě o pronájmu – Podmínky užívání systému

Příloha specifikuje základní podmínky užívání systému nájemce.

Nájemce zabezpečí provoz systému v souladu s provozním řádem systému

Nájemce se zavazuje ve vztahu ke kvalifikaci osob postupovat v souladu s účelem užití předmětu nájmu a dle dále uvedených pravidel:

Nájemce nepřidělí přístupová práva k systému osobám, které nejsou s nájemcem v pracovně právním nebo služebním poměru.

Nájemce nepřidělí přístupová práva k systému osobám, které neabsolvovali školení odpovídající jejich pracovnímu nebo služebnímu zařazení

Nájemce přidělí vyškoleným osobám přístupová práva pouze v rozsahu jimi absolvovaného školení.

Nájemce zabezpečí lokální a vzdálené datové komunikační služby minimálně na úrovni specifikace uvedené v článku 13 smlouvy. Datová síť bude splňovat minimálně následující parametry:

Centrální část systému je dimenzována ta, aby doba odezvy na uživatelský vstup byla do 3 vteřin v měřícím bodě. Měřícím bodem se rozumí koncová stanice s požadovanými parametry výkonu a nastavení, která bude nezávislá na provozu WAN sítí nájemce a bude připojena na LAN centrálního systému, tj. v kterémkoli místě centrálního systému před napojením na firewall nájemce. Pro výše uvedenou dobu je dimenzována serverová část systému včetně interní sítě systému.

Průchodnost WAN sítí musí být minimálně taková, aby zabezpečila pro každého aktivního uživatele odpovídající komunikační kanál.

Požadovaná šířka komunikačního kanálu pro:

standardní SAPGUI – 5 kb/s

standardní WEB - 10 kb/s

Pro tisk je v průměru požadován komunikační kanál o šíři 4/kb/s.

7.3 Požadavek pronajímatele na ochranu osobních dat (čl. 21 smlouvy o pronájmu systému)

Pronajímatel poskytuje nájemci systém za účelem užívání a není a nesmí být v žádném případě považován za provozovatele systému ani za zpracovatele dat nájemce ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů.

Nájemce je odpovědný za to, že)a) bude užívat systém v souladu se zákonem č. 101/200 Sb. a že)b) provede potřebná fyzická a organizační opatření k tomu, aby osobní údaje byly chráněny v souladu s tímto zákonem.

Pronajímatel bude za účelem ochrany osobních dat nájemce dodržovat fyzická a organizační opatření nájemce, se kterými byl prokazatelně seznámen.

Z výše uvedených ustanovení smlouvy vyplývá, že ochrana osobních údajů ve smyslu zákona 101/2000 Sb. je plně v kompetenci Ministerstva vnitra ČR. Ministerstvo vnitra zodpovídá v plném rozsahu za ochranu osobních údajů.

Řešení přístupu pronajímatele do systému EKIS

Při řešení přístupu pracovníků pronajímatele do systému je nutné rozlišovat, zda se jedná o systém produktivní, testovací nebo vývojový.

7.4 Přístup pronajímatele do vývojového a testovacího systému EKIS

V těchto systémech nejsou skutečná data, pouze nasimulovaná, testovací.

Pracovníci a smluvní partneři pronajímatele mají přístup do vývojových a testovacích systémů na základě žádosti o zavedení do výše uvedených systémů po celou dobu platnosti smlouvy o pronájmu systému. Tato žádost musí být schválena ředitelem projektu za stranu pronajímatele i za stranu nájemce. Pracovníci pronajímatele přistupují do těchto systému na svoje uživatelské ID.

7.5 Přístup pronajímatele do produktivního systému EKIS

Pracovníci pronajimatele přistupují v nutných případech do produktivního systému na základě níže uvedených pravidel:

Pracovník pronajimatele – konzultant musí splňovat tyto podmínky:

Musí mít prověření na stupeň utajení VYHRAZENÉ nebo DŮVĚRNÉ a zúčastňuje se 1x ročně půldenního školení bezpečnosti EKIS.

Na základě žádosti podané na formuláři „Žádost o přístup pracovníka pronajímatele na produktivním systému“ (vzor formuláře je uveden v příloze) mu bude umožněn přístup do produktivního systému EKIS a to na dobu uvedenou v tomto formuláři. Pracovník nájemce uvedený v tomto formuláři je povinen vykonávat dozor nad činností pracovníka pronajímatele po celou dobu jeho přístupu do produktivního systému.

Kompetentní pracovník nájemce umožní přístup pracovníku pronajímatele na základě řádně vyplněného a podepsaného formuláře a sdělí mu vstupní heslo.

Ukončení práce oznámí pracovník pronajímatele správci uživatelů nebo jinému kompetentnímu pracovníkovi nájemce a ten provede nebo zařídí neprodleně zablokování daného účtu uživatele v produktivním systému a učiní o tom záznam v příslušném formuláři.

8 UŽIVATELÉ EKONOMICKÉHO INFORMAČNÍHO SYSTÉMU MV ČR

V současné době využívá systém EKIS 9.885 pracovníků rezortu ministerstva vnitra. Jejich přístup do systému se liší podle pracovního zařazení. Pracovníci, kteří provádějí modifikaci a zakládání pohyblivých dat přistupují do systému prostřednictvím klienta SAP GUI. Vedoucí pracovníci rezortu využívají zprostředkovaný přístup pomocí WEB aplikace.

Typ uživatele	Způsob připojení do systému EKIS	Počet
Účetní, personalisté, materialisté	SAPGUI	1960
Vedoucí pracovníci PČR a jejich zástupci	WEB aplikace LOTUS Domino	7925
CELKEM		**9885**

tabulka č. 2 : Počet uživatelů EKIS

8.1 Způsob přístupu do systému

Uživatelé přistupují do systému:

Přímý přístup do SAP R/3 prostřednictvím klienta SAP GUI

Na pracovní stanici je nainstalován tzv. tenký klient – SAP GUI, který prostřednictvím sítě EKISNET a protokolem TCP/IP komunikuje s aplikačním serverem. Předpokládá se přímé spojení mezi pracovní stanicí a aplikačním serverem. Aplikační servery přistupují pomocí stítě LAN k jednomu databázovému serveru, na kterém je uložena veškerá data aplikace.

SAP GUI realizuje tzv. prezentační část architektury. Znamená to, že zobrazuje data ze serveru, nebo zprostředkovává jejich vstup. Na klientské stanici se neukládají žádná data aplikace, jsou zde pouze soubory reprezentující klienta SAP GUI.

přístup pomocí WEB aplikace LOTUS Domino

Přístup do systému je zprostředkován WEB aplikací LOTUS DOMINO, jedná se o naprogramovanou aplikaci, která je schopna komunikovat s aplikacemi SAP R/3

Rozdíl mezi přímým vstupem:

Aplikace je provozována off-line.

Funkce aplikace nejsou bezprostředně závislé na dostupnosti serveru/sítě

Data jsou ukládána lokálně a následně jsou replikována do centrálního serveru LOTUS DOMINO, který zprostředkovává automatické zaúčtování do systému SAP R/3.

8.2 Autentizace uživatele

Autentizaci uživatelů označujeme také jako verifikaci. Jedná se o potvrzování, ověřování správnosti, proces ověřování identity uživatele. Uživatel zadá svoji identitu a umožní její ověření. Ověřovaný subjekt předloží tvrzení o své identitě, na základě předložené identity se srovnají aktuální charakteristiky s uloženými charakteristikami, které této identitě odpovídají v záznamech identifikační databáze.

V současné době se v informačních systémech využívají tři základní metody autentizace uživatelů, nebo kombinace dvou či všech tří metod

Metody autentizace uživatelů:

Co daný uživatel zná

Informace, např. PIN, heslo, přístupová fráze. Znalost, kterou lze přenášet do systému. Autentizace touto metodou je snadná a nevyžaduje složitou údržbu. Ale informace může být snadno zjištěna, i bez vědomí uživatele. Uživatel může informaci zapomenout.

Co daný uživatel má

Fyzický objet, v této souvislosti označovaný jako TOKEN. Jedná se například o přístupovou kartu. Token lze obtížně kopírovat, ztráta je zjistitelná. Nevýhodou je špatná kompatibilita, možnost poškození tokenu.

Podmínkou použití je existence čtecího zařízení.

Co daný uživatel je

Biometrická informace, např. otisk prstu.

Jedná se o část těla, či určitou charakteristiku osoby, která se v čase buď vůbec nemění, nebo se mění jen velmi omezeně. Výhodu je, že nelze nic zapomenout či ztratit. Nevýhodou je, že přesné měření biometrických informací je velmi obtížné. Přesnost měření ovlivňuje celkovou bezpečnost systémů.

V ekonomickém informačním systému MV je aplikována metoda **„Co daný uživatel zná“**. Systém ověřuje totožnost uživatele standardně pomocí uživatelského jména a hesla. Použitá hesla nejsou uložena v databázi, je tam uložen pouze jejich otisk vytvořený jednosměrným hash algoritmem. Přenos hesla mezi klientem a serverem probíhá v nečitelném tvaru. Při použití hesel, jsou stanovena pravidla pro tvorbu hesel, která jsou vynucována při přihlašování uživatele do systému, nebo při změně jeho hesla.

Použití hesel se řídí těmito pravidly:

Minimální délka hesla.

Zákaz zadávání hesla s diakritikou.

Maximální doba platnosti hesla. Po uplynutí stanovené doby, je uživatel vyzván ke změně hesla.

Zákaz použití prvních tří znaků ze jména uživatele.

Zákaz použití křestních jmen.

Změnu hesla může uživatel provést pouze 1x za den. Administrátor může na základě písemné žádosti uživatele provést změnu hesla kdykoliv. Postup žádosti uživatele o změnu hesla je popsán v provozním řádu EKIS.

Při provádění změny hesla se nové heslo musí lišit od pěti předchozích hesel alespoň v jednom znaku.

K preventivním opatřením proti neautorizovanému přístupu se řadí:

Systém denně kontroluje u všech uživatelů prostřednictvím jejich kmenových dat v modulu personalistika a mzdy, zda jejich pracovní poměr v rezortu není ukončen. V případě ukončení pracovního (služebního) poměru je příslušný uživatelský účet automaticky zablokován.

Při X chybných přihlášeních se účet uživatele zamkne. Účet může odemknout na základě písemné žádosti jen administrátor nebo pracovník HOT LINE EKIS.

Systém pravidelně ověřuje funkčnost spojení mezi serverem a klientem, pokud je spojení přerušeno dojde k automatickému ukončení těch činností uživatele, které byly vyvolány před rozpojením. Činnosti, které byly předem naplánovány, a byly spuštěny jako úloha na pozadí, zůstávají zachovány.

Při delší nečinnosti klávesnice dojde k automatickému odhlášení uživatele. Doba nečinnosti je nastavena na serveru a uživatel jí nemůže ovlivnit. Zde je nevýhodou, že práce v poště EKIS je považována za nečinnost. Při zasílání informací většího rozsahu hrozí nebezpečí, že bude uživatel odhlášen.

Je zakázáno duplicitní přihlášení do systému.

Veškeré přístupy uživatelů do systému a jejich aktivita je zaznamenávána do „log souborů“, systému umožňuje jejich analýzu.

Z důvodu bezpečnosti EKIS probíhá monitorování systému a provádí se záznam činnosti každého uživatele. Z těchto důvodů musí každý uživatel do systému přistupovat na svoje uživatelské ID, aby se dala následně jeho činnost v systému vyhodnotit.

Přidělení přístupového oprávnění do EKIS se řídí stanoveným postupem. Bez jeho dodržení nelze z bezpečnostních důvodů přístup do EKIS zřídit.

8.3 Podmínky přidělení přístupu do systému EKIS

- Podání řádně vyplněné a schválené žádosti o zřízení přístupu do EKIS na předepsaných formulářích.

- Absolvování těchto školení:

Odborné školení podle modulů a r rolí požadovaných na formuláři o zřízení přístupu do EKIS.

Školení bezpečnosti dat v EKIS a podepsání „Poučení o bezpečnosti a ochraně dat“ a „Prohlášení o ochraně dat ve smyslu zákona 101/200 Sb. ve znění pozdějších předpisů“, které se zakládají do personálního spisu (Příloha).

Schválení žádosti se provádí na více úrovních a to podle vlastníka dat:

- Přístup na vlastní personální oblast (organizační jednotka) schvaluje žadatel, tj. primární vlastník dat – ředitel s personální pravomocí organizačního celku.

- Přístup přes více organizačních jednotek je nutné postoupit žádost pracovišti kompetenčního centra cestou sekundárního vlastníka dat, tj. ředitel personálního odboru MV ČR.

- Přístup k datům vybraných útvarů podléhá schválení ředitelem dotčeného útvaru.

Postup při přidělení, změně nebo odnětí oprávnění do EKIS (jednotlivé formuláře jsou předloženy v příloze):

- Nadřízený s personální pravomocí budoucího uživatele (žadatel) předkládá na předepsaném formuláři žádost o zavedení uživatele do EKIS kompetenčnímu středisku. V případě, kdy je požadován přístup přes více organizačních jednotek, je nutné schválení sekundárním vlastníkem dat.

- Uživatel musí být řádně proškolen a absolvovaná školení musí být zaznamenána na žádosti o zavedení uživatele do EKIS .

- Kompetenční středisko na základě žádosti podepsané uživatelem žadatelem (popř. sekundárním vlastníkem dat), bezpečnostním správcem EKIS a školitelem ovládání systému, provede zavedení (doplnění uživatelské role, zrušení oprávnění) uživatele do produktivního systému EKIS.

8.4 Autorizační koncept a přístup k informacím

Autorizace uživatelů je proces přiřazení oprávnění pro práci v systému, který specifikuje, co uživatel může v systému vykonávat, přiřazuje uživatelská oprávnění. Autorizace je prováděna na základě identity a bezpečnostní politiky. Jde o proces, který obvykle následuje po autentizaci.

Příkladem autorizace uživatelů je autorizační koncept a přístup k informacím v Ekonomickém informačním systému Ministerstva vnitra ČR, který se řídí těmito pravidly:

Vlastní systém autorizace probíhá na úrovni aplikační vrstvy, ta je zajištěna na základě uživatelských dat. Přístup ke konkrétním informacím je zprostředkován pomocí aplikačních programů.

Na základě přihlášení uživatele je nalezen jeho exkluzivně definovaný účet, který musí být v systému předem exklusivně definován. Uživateli jsou přiděleny uživatelské role, které obsahují profily, jimiž je stanoveno příslušné oprávnění. Profily obsahují autorizační objekty, které obsahují pole s hodnotou, a nebo množiny hodnot, které určují povolení přístupu k definovanému objektu nebo jeho vyloučení (možnost explicitní definice cestou povolení hodnot, nebo zákazem hodnot).

Systém umožní realizovat odlišné oprávnění pro různé skupiny pracovníků. V extrémním případě je možné nastavit pro každého uživatele přístup k odlišným informacím.

Objektově orientovaná architektura bezpečnosti EKIS umožňuje regulovat přístupová práva k jednotlivým objektům (nejenom ke statickým datům, ale například i k funkcím).

Každý přístup k datům může být proto mezen nejenom množinou hodnot, ale i dynamicky, t.j. funkcemi. Znamená to, že každému uživateli lze definovat, zda uživatel data vytváří, modifikuje, čte nebo určitá data nemá přístupná.

Udělením oprávnění se definuje, se kterými objekty uživatelé mohou v systému pracovat a jaké činnosti s nimi mohou vykonávat. Udělování oprávnění se uskutečňuje v několika krocích:

určení přípustné hodnoty oprávnění pro jednotlivé objekty

sloučení několik oprávnění do profilu (popřípadě do skupin profilů),

přiřazení profilu oprávnění uživateli (několik profilů).

Na základě analýzy činností každého uživatele systému byl definován rozsah oprávnění a byly navrženy typové role pro jednotlivé činnosti.

Shrneme-li způsob řešení autorizace v EKIS, tak pro každý objekt oprávnění jsou nutné dva údaje:

Seznam útvarů, pro které je možné kmenová data zpracovávat,

Seznam činností, které jsou přípustné při zpracování dokladů v uvedených útvarech.

Pomocí této kombinace je možné povolené činnosti dobře diferencovat. Pokud chce oprávněný uživatel provést nějakou činnost, systém ověří, zda smí provést činnost pro uvedené organizační jednotky a zda vlastní požadovaná funkční oprávnění. Tato ověření se provádí vždy po vložení dat uživatele. Jsou-li všechna ověření oprávnění úspěšná, lze provést další pracovní krok.

Příklad rolí definovaných pro EKIS II	
OBLAST PERSONALISTIKY	
Personalista	Provádí všechny úkony související s personalistikou
Personalista náborář	Provádí nábor nových pracovníků
OBLAST ODMĚŇOVÁNÍ	
Vedoucí mzdové účtárny	Provádí zúčtování mezd a platů, obsahuje roli Mzdový účetní
Mzdový účetní	Zpracovává mzdovou agendu
Pracovník sociálních evidencí	Zpracovává agendu týkající se sociálního zabezpečení

tabulka č. 3 Příklad rolí definovaných pro EKIS II

Na základě požadavků útvarů jsou vytvářena i speciální přístupová oprávnění. Například pracovnice HOTLINE mají omezený přístup do kmenových dat zaměstnanců MV (organizační přiřazení, plán služeb, přesčasů, pohotovostí, nepřítomností).

Pro analytiky útvarů bylo vytvořeno oprávnění s možností vytěžovat informace k vytváření přehledu čerpání mzdových prostředků apod.

V poslední době jsem řešila v souvislosti s účinností zákona 187/2006 Sb., o nemocenském pojištění žádost odboru sociálního zabezpečení MV o vytvoření registru pojištěnců. Odbor sociálního zabezpečení MV je orgánem sociálního zabezpečení pro policisty.Pověřené pracovnici odboru byla vytvořena možnost nahlížet do kmenových dat policistů ale pouze v omezeném rozsahu (dle požadavku zákona 187/2006 Sb.).

Zákon dále požaduje umožnit ostatním orgánům sociálního zabezpečení nahlížet do registru pojištěnců MV. Tento požadavek nebyl splněn. Na základě jednání s Ministerstvem práce a sociálních věcí ČR nám byla udělena výjimka a přislíbena změna zákona. V současné době není systém SAP uzpůsoben uživatelským přístupům mimo rezort MV.

Samostatným okruhem uživatelů jsou přístupová práva ve WEB aplikace LOTUS DOMINO:

Použitý server LOTUS DOMINO obsahuje autentizací modul, který zabezpečuje definici přístupových práv a zabezpečení komunikace. V aplikaci LOTUS DOMINO se přidělují přístupová práva podle přidělené role a přístup na organizační jednotku se odvíjí od toho, kde je pracovník zařazen (kmenová data pracovníka). Při změně zařazení pracovníka na jinou organizační jednotku nebo při ukončení služebního (pracovního) poměru, ztrácí pracovník automaticky přístup k jakýmkoliv datům. Např. při změně systemizace útvaru, dojde ke změně organizační jednotky v kmenových datech pracovníka, ale uživatelský účet byl zřízen na původní organizační jednotku. V tomto případě je nutno na základě písemné žádosti oprávnění upravit.

Tato oprávnění umožňují veliteli/vedoucímu (nebo pověřenému pracovníkovi) zaslat do systému SAP R/3 cestou rozhraní WEB např. plán služeb, čerpání služebního/pracovního volna, evidenci přesčasů a pohotovostí. V omezené míře velitel může využívat pomocí sestav pro velitele zpětnou vazbu ze systému SAP R/3.

Příklad sestav pro oblast odměňování:

Proplacené hodiny příplatků v hodinách

Proplacené hodiny příplatků v Kč

Proplacené hodiny příplatků na zakázku v hodinách

Proplacené hodiny příplatků na zakázku v Kč

Rekapitulace – mzdy

Rekapitulace – služební příjmy

Udělené peněžité odměny

Výkaz příplatků

Výkaz hodin – sl. poměr

Osobní příplatky – porovnání růstu

Nevybrané NV za předchozí 3 měsíce

Evidence pracovní doby

Evidence pracovní doby – detailní

Přehled práce/nepřítomností/přesčasů/pohotovostí

Přehled čerpání limitních přesčasů

Rekapitulace FPD

Rekapitulace FPD – loňský rok

Rekapitulace FPD – převod vyšší než 10% NFPD

Katalog uživatelských rolí EKIS WEB	
Název uživatelské role	**Technický název role/pravomoc**
Vedoucí zaměstnace - vedoucí odboru, vedoucí oddělení, ředitel (územního) odboru	Velitel/vedoucí s kázeňskou pravomocí
	plánování služeb
	evidence přítomností a nepřítomností
	plnění kvalifikačních požadavků a návrh na výcvik
	plná funkcionalita WEB aplickace
Operační - referent operačního střediska, operační důstojník	Operační důstojník
	Přehled osob se základními osobními údaji
Služební lékař	Služební lékař
	záznam preventivní prohlídky, očkování
Plánovač	Plánovač
	plánování služeb
	evidence přítomností a nepřítomností
	přístup pouze k apletu "Časové plánování"
Dočasný vedoucí zaměstnanec	Velitel/vedoucí mimo hierarchii
	Stejná oprávnění jako velitel
	Na základě žádosti je nastaveno propojení umožňuje přístup i na jednotky, které neodpovídají jeho pracovnímu/služebnímu zařazení.
Bezpečnostní referent	Bezpečnostní referent
	Návrhy změn k údajům BP a BZ

tabulka č.4 :Katalog uživatelských rolí EKIS WEB

9 MOŽNÉ PROBLÉMY A JEJICH ŘEŠENÍ

Ekonomický informační systém byl nastaven na základě provedené analýzy bezpečnostních rizik, jejíž výsledky byly definovány ve smlouvě mezi IBM, s.r.o a ministerstvem vnitra. Proto nedochází k závažným problémům v oblasti bezpečnosti i v oblasti ochrany osobních údajů.

Po dobu provozu byly zjištěny některé nedostatky vyplývající z daného rozsahu a počtu uživatelů.

V případě, že pracovník ukončil pracovní (služební) poměr v rezortu ministerstvu vnitra, nebyla tato skutečnost včas nahlášena kompetenčnímu středisku, které vede evidenci uživatelů, a uživatelský účet byl nadále užíván novým pracovníkem, který nastoupil na pozici původního pracovníka. Tento zaměstnanec neměl ještě zřízený svůj uživatelský účet. Nyní je každý den prováděna automatická kontrola uživatelských účtů s aktuálním stavem v personalistice (kmenových datech uživatelů). V případě ukončení pracovního/služebního poměru je automaticky zablokován příslušný uživatelský účet.

Ze strany bezpečnostních správců je nutné klást větší pozornost na dodržování bezpečnostních předpisů uživateli, zejména kontrolovat uživatele při manipulaci s tiskovými výstupy. V této souvislosti je nutno minimálně jedenkrát ročně provádět doškolování uživatelů v bezpečnosti informačního systému EKIS. Bezpečnostní správci jsou minimálně jedenkrát ročně proškolováni pracovníky kompetenčního centra (bezpečnostní manažer).

10 OCHRANA OSOBNÍCH ÚDAJŮ – SPRÁVNÍ DELIKTY/SANKCE

Správní delikty při porušení ochrany osobních údajů řeší hlava VII zákona 101/2000 Sb., o ochraně osobních údajů

Výpis ze zákona č. 101/2000 Sb.:

„§ 44

Fyzická osoba, která

je ke správci nebo zpracovateli v pracovním nebo jiném obdobném poměru,

vykonává pro správce nebo zpracovatele činnost na základě dohody, nebo

v rámci plnění zvláštním zákonem uložených oprávnění a povinnosti přichází u správce nebo zpracovatele do styku s osobními údaji,

se dopustí přestupku tím, že poruší povinnost mlčenlivosti

Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů

nestanoví účel, prostředky nebo způsob zpracování nebo stanoveným účelem zpracování poruší povinnost nebo překročí oprávnění vyplývající ze zvláštního zákona,

zpracovává nepřesné osobní údaje,

shromažďuje nebo zpracovává osobní údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu

uchovává osobní údaje po dobu delší než nezbytnou k účelu zpracování

zpracovává osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně

neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem,

odmítne subjektu údajů poskytnout požadované informace,

nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů,

nesplní oznamovací povinnost podle tohoto zákona.

Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů některým ze způsobů podle odstavce (2)

ohrozí větší počet osob svým neoprávněným zasahováním do soukromého a osobního života, nebo

poruší povinnosti pro zpracování citlivých údajů.

Za přestupek podle odstavce 1 lze uložit pokutu do výše 100 000 Kč.

Za přestupek podle odstavce 2 lze uložit pokutu do výše 1 000 000 Kč.

Za přestupek podle odstavce 3 lze uložit pokutu do výše 5 000 000 Kč.

§44a

Právnická osoba nebo fyzická osoba podnikající podle zvláštních předpisů se jako správce nebo zpracovatel dopustí správního deliktu tím, že při zpracování osobních údajů

nestanoví účel, prostředky nebo způsob zpracování, nebo stanoveným účelem zpracování poruší povinnost nebo překročí oprávnění vyplývající ze zvláštního zákona,

zpracovává nepřesné osobní údaje

shromažďuje nebo zpracovává osobní údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu,

uchovává osobní údaje po dobu delší než nezbytnou k účelu zpracování,

zpracovává osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně

neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem

odmítne subjektu údajů poskytnou požadované informace,

nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů,

nesplní oznamovací povinnost podle tohoto zákona.

Právnická osoba jako správce nebo zpracovatel se dopustí správního deliktu tím, že při zpracování osobních údajů některým způsobů podle odstavce 1

ohrozí větší počet osob svým neoprávněným zasahováním do soukromého a osobního života nebo

poruší povinnosti pro zpracování citlivých údajů

Za správní delikt podle odstavce 1 se uloží pokuta do výše 5 000 000 Kč.

Za správní delikt podle odstavce 2 se uloží pokuta do výše 10 000 000 Kč.

§45a

Právnická osoba nebo podnikající fyzická osoba se dopustí správního deliktu tím, že poruší zákaz zveřejnění osobních údajů stanovený jiným právním předpisem.

Za správní delikt podle odstavce 1 se uloží pokuta do 1 000 000 Kč.

Za správní delikt podle odstavce 1 spáchaný tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem se uloží pokuta do 5 000 000 Kč.“

Výpis ze zákona 101/2006 Sb., o ochraně osobních údajů uvádím, aby bylo patrné, že v případě porušení ustanovení zákona jsou sankce velmi vysoké. Jsou daleko vyšší než sankce vyplývající z porušení ustanovení jiných zákonů (utajované informace, bezpečnost práce,…..).

Na Ministerstvu vnitra ČR za dobu ostrého provozu Ekonomického informačního systému nebylo nutné přistoupit na tyto sankce, a to jak u fyzických osob (uživatelé EKIS), tak i právnických osob (útvary MV). Vyskytla se drobná porušení bezpečnostních pravidel (např. dostupné heslo, pokusy o neautentizovaný přístup), která byla řešena kázeňským postihem nebo domluvou. K úniku osobních údajů nedošlo.

11 PŘEDPOKLÁDANÝ VÝVOJ V PROBLEMATICE OCHRANY OSOBNÍCH ÚDAJŮ

V roce 1995 začaly vznikat první představy změny dosavadních informačních systémů v Ministerstvu vnitra. Stávající různorodé aplikace nebyly nijak provázány. Zvlášť se provozoval systém účetnictví, platy, služební příjmy, evidence majetku. Nejenom, že systém nebyl provázán, ale nebyla koncepčně řešena bezpečnost informačních systémů, přístupová oprávnění, složitým způsobem se prováděly distribuce nových verzí. Existovalo zde jakési kompetenční centrum, kde pracovali autoři aplikací. V případě, že byla aplikace vytvořena externím pracovníkem, byl stanoven zaměstnanec MV k správě této aplikace. Toto centrum působilo pouze jako podpora uživatelů.

V roce 1999 byl zahájen produktivní provoz systému EKIS I (účetnictví). Systém, kterým jsem se ve své práci zabývala, EKIS II (personalistika a mzdy) byl uveden do produktivního provozu 1. října 2003. Problematika mzdových agend samostatně zahájila ostrý provoz 1.1.2004. U obou systémů je možnost vzájemného propojení. Při zpracování mezd dochází přenosu převodních příkazů a účetních dokladů ze systému EKIS II do systému EKIS I. Ale na EKIS I a EKIS II jsou uzavřené samostatné smlouvy.

V případě „Personalistiky a mezd“ byla uzavřena smlouva na 5 let a již dvakrát byla dodatkem ke smlouvě prodloužena na 18 měsíců. Naposledy v dubnu 2011.

Vzhledem k takto krátkému období, na které byla smlouva prodloužena, a současným „silným“ bezpečnostním opatřením se neuvažuje o jiném řešení bezpečnosti.

Doporučovala bych posílit proškolování oprávněných uživatelů a jednotlivých bezpečnostních správců v oblasti bezpečnosti informačního systému s důrazem na problematiku ochrany osobních údajů.

S vývojem informačních technologií přicházejí i nové technologie v oblasti bezpečnosti. Jedná se např. o principy slabé a silné autentizace uživatelů :

hesla (jejich ukládání) a jednorázová hesla

autentizace tokeny

biometrik

vícefaktorová autentizace

certifikáty

protokoly výzva-odpověď a eskalační protokoly

Dochází k vývoji v problematice bezpečného hardware – vnitřní architektura, bezpečnostní požadavky na kryptografické moduly.

ZÁVĚR

Ekonomický informační systém MV splňuje základní bezpečnostní požadavky v oblasti počítačové bezpečnosti, včetně požadavků kladených na ochranu osobních údajů:

Jednoznačná autentizace uživatele

Ochrana důvěrnosti a integrity autentizační informace

Volitelné řízení přístupu k objektům na základě rozlišování a správy přístupových práv oprávněného uživatele a identity uživatele nebo jeho členství ve skupině uživatelů

Nepřetržité zaznamenávání událostí, které mohou ovlivnit bezpečnost informačního systému

Zabezpečení auditních záznamů před neautorizovaným přístupem

Záznam použití autentizačních informací Záznam pokusů o zkoumání přístupových práv, vytváření nebo rušení objektu nebo činnost autorizovaných uživatelů ovlivňující bezpečnost informačního systému

Možnost zkoumání auditních záznamů a stanovení odpovědnosti jednotlivého oprávněného uživatele informačního systému

Ošetření paměťových objektů před jejich dalším použitím, zejména před přidělením jinému subjektu, které znemožní zjistit jejich předchozí obsah

Zajištění ochrany důvěrnosti dat během přenosu

Při psaní bakalářské práce jsem z velké části čerpala z materiálů, které mi byly poskytnuty pracovištěm bezpečnostního manažera ekonomického informačního systému. Vzhledem k tomu, že tyto materiály obsahovaly vyčerpávající souhrn informací o zabezpečení bezpečnosti EKIS, včetně ochrany osobních údajů, neprováděla jsem výzkum na jednotlivých útvarech Ministerstva vnitra ČR. V bakalářské práci jsem využila i vlastních zkušeností. Na Ministerstvu vnitra ČR pracuji jako projektant informačních systémů. V Ekonomickém informačním systému zodpovídám za oblast odměňování a sociálních evidencí, především za správnost nastavení systému. Součástí mé pracovní

náplně je i odborná podpora všem mzdovým účetním a referentům sociální evidence. Problematika ochrany osobních údajů se promítá i do mého zaměstnání.

ZÁVĚR V ANGLIČTINĚ

The Economic Information System of Ministry of Interior complies with basic security requirements in scope of computer security including personnel information security requirements:

- Explicit user authentization
- Confidentiality protection and authentication information integrity
- Optional object access control based on differentiation and authorized user access permitions administration, and user identity or their membership in group of users.
- Continual recording of events which can influence information system security.
- Auditor records security against unauhorized access
- Recording of authentication information application
- Recording of attempts to inspect access permitions, generation or cancelling of an object, or activity of authorized users affecting security of information system
- Possibility to inspect auditor records and to determine resposibility of individual authorized user of information system
- Handling of memory objects prior to their next use, especially prior to assigning to another subject, which forbids to detect their previous content
- Ensuring data security during transmission

For writing Bachelor Thesis materials which were provided by department of security manager of the Economic Information System. The materials contained comprehensive information about security of EKIS, including protection of personnel information, so I did not do any research at individual subdivisions of Ministry of Interior of the Czech Republic.

I also used my own practical experience in the Bachelor Thesis.

I am employed as information systems designer at Ministry of Interior. In the Economic Information System I am responsible for remuneration section and social records section, especially for precise configuration of the system.

Part of my workload is also expert support for all wage accountants and social records officers. One part of my profession is personnel data security.

SEZNAM POUŽITÉ LITERATURY

[1] Zákon 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů ze dne 4. dubna 2000,zákon vyhlášen 25. 4. 2000 ve Sbírce zákonů v částce 32 pod číslem 101/2000 Sb.

[2] Kolektiv autorů.Autentizace uživatelů a autorizace elektronických transakcí, příručka manažera.Vydáno TATE International, s.r.o., v Praze v listopadu 2007 ISBN 978-80-86813-14-1.

[3] JUDr. Vladimír Laucký.Řízení technologických procesů v průmyslu komerční bezpečnosti.Vydáno Univerzitou Tomáše Bati ve Zlíně v čevrnu 2006 ISBN 80-7318-432-X.

[4] JUDr. Vladimír Laucký.Technologie komerční bezpečnosti I.Vydáno Univerzitou Tomáše Bati ve Zlíně v roce 2010 ISBN 978-80-7318-889-4.

[5] JUDr. Vladimír Laucký.Technologie komerční bezpečnosti II.Vydáno Univerzitou Tomáše Bati ve Zlíně v roce 2007 ISBN 978-80-7318-631-9.

[6] JUDr. MgA. Michal Šalomoun, e-kniha Ochrana osobních údajů v teorii i praxi. Autorská práva k dílu vykonává společnost Metamorfózy, s.r.o., se sídlem: Bráfova tř. 770/52, Třebíč, IČ: 27730361, zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně v oddílu C, vložce č. 55178.

[7] Materiály zpracované Ministerstvem vnitra ČR

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

EKIS	Ekonomický informační systém Ministerstva vnitra ČR
	EKIS II – Ekonomický informační systém zaměřený na personalistiku a mzdy
TCP/IP	Informační sítě – protokolová sada
SAP GUI	Uživatelský klient

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

I. Žádost o přístup pracovníka pronajímatele do systému SAP/R3

II. Prohlášení o poučení o povinnostech „uživatele dat“ dle zákona č. 101/2000 Sb.

III. Poučení o bezpečnosti a ochraně dat v systému EKIS

IV. Žádost o zřízení oprávnění přístupu do systému EKIS pro uživatele

V. Žádost o změnu nebo doplnění oprávnění přístupu do systému EKIS pro uživatele

VI. Žádost o zrušení oprávnění přístupu do systému EKIS

PŘÍLOHA P I: ŽÁDOST O PŘÍSTUP PRACOVNÍKA PRONAJÍMATELE DO SYSTÉMU SAP/R3

Žádost o přístup pracovníka pronajímatele do systému SAP/R3

Údaje pracovníka: *Účast pracovníka MV:*

Firma:	Odbor:
Jméno:	Jméno:
Příjmení:	Příjmení:
Tel:	Tel:
Podpis:	OEČ:
Předloženo dne:	Doba dohledu: Stále

Rozsah požadovaného oprávnění: ……SAP_ALL……

……

Doba oprávnění: ode dne : čas:

do dne : čas:

Systém*): **O** HR2 klient:……..…..

Systém*): **O** HR3 klient:…….…….…..

Systém*): **O** MV2 klient:……..…..

Systém*): **O** MV3 klient:……..…..

Jméno (popř. OEČ) pro zavedení :

Inicializační heslo: nechat původní

Schválil Ředitel projektu EKIS II:

…….. ……dne: ……..

Schválil Ředitel projektu EKIS I:

…….…….. dne: ……..

PŘÍLOHA P II: PROHLÁŠENÍ O POUČENÍ O POVINNOSTECH UŽIVATELE DAT DLE ZÁKONA Č. 101/2000 SB.

Číslo jednací:

Počet stran: 1

Výtisk číslo:

Prohlášení

Prohlašuji, že jsem byl poučen o povinnostech „uživatele dat“ dle zákona č. 101/2000 Sb.,

o ochraně osobních údajů, a o povinnostech „uživatele dat“ dle Nařízení Ministerstva vnitra

č. 20/2007, o personální evidenci, v rozsahu nezbytném pro bezpečnost a ochranu dat v systému EKIS.

Jméno pracovníka: …… Školení

provedl:……..

OEČ: ……

Podpis: …… Podpis: ……..

Datum: …… Datum: ……..

Výtisk č. 1 obdrží pracovník

Výtisk č. 2 založit do personálního spisu

Výtisk č. 3 přiložit k žádosti o zřízení oprávnění přístupu do systému EKIS

PŘÍLOHA P III: POUČENÍ O BEZPEČNOSTI A OCHRANĚ DAT V SYSTÉMU EKIS

Číslo jednací:

Počet stran: 2
Výtisk číslo:

Poučení o bezpečnosti a ochraně dat v systému EKIS

Podle Provozního řádu EKIS – příručka 24 a podle zákona č. 101/2000 Sb. o ochraně osobních údajů, musí být každý uživatel poučen o ochraně dat v systému EKIS v souladu s následujícími body:

1) Systém EKIS je určen pro potřeby pracovníků MV ČR k plnění pracovních povinností určených vedoucími funkcionáři a správcem systému EKIS. Činnost každého uživatele, z hlediska bezpečnosti, podléhá kontrole ze strany správce systému EKIS, administrátora a bezpečnostního správce.
2) Žádný uživatel nesmí provádět takovou činnost,
   a) která by poškodila nebo by mohla poškodit informace nebo procesy systému EKIS (z hlediska ztráty, neoprávněná modifikace dat, poškození dat a nebo poškození systému včetně jeho nastavení aj. ..)
   b) která by byla nebo mohla být škodlivá pro Ministerstvo vnitra (vyzrazení dat, zneužití osobních údajů aj….)
3) Každý uživatel:
   a) musí heslo uchovávat v tajnosti, tzn. nesdělovat ho druhé osobě s výjimkami osob uvedených v Provozním řádu systému EKIS a po ukončení činnosti těchto osob heslo neprodleně změnit;
   b) vstupní heslo do pracovní stanice může sdělit pouze pro servisní účely provoznímu programátorovi nebo zástupci pronajímatele, který má podepsanou dohodu mlčenlivosti. Jakmile takový pracovník ukončí svou servisní činnost, musí heslo neprodleně změnit.
4) Hesla:
   Heslo do všech aplikací systému EKIS (SAP R/3, Lotus Notes popř. WEB):
   a) se musí volit náhodně a nesmí se odvozovat od již použitých hesel. Rovněž se nesmí volit hesla jednoduchá a lehce zjistitelná (odvozená od mého jména nebo mých rodinných příslušníků, data narození, okolních předmětů atd.),
   b) musí obsahovat minimálně 6 alfanumerických znaků, s min. 1 numerickým znakem, bez numerického znaku na prvním a posledním místě hesla (v případě Lotus Notes je to 8 znaků),
   c) uživatel pracovní stanice má za povinnost měnit hesla v intervalu ne delším než dva měsíce, administrátor (správce) nebo bezpečnostní správce každý měsíc,
   d) heslo je vždy nutné okamžitě změnit, když existuje podezření, že bylo (nebo mohlo být) prozrazeno. Prozrazení hesla, nebo své podezření neprodleně a prokazatelně (písemně) oznámit bezpečnostnímu správci a svému nadřízenému pracovníkovi.
5) Veškeré činnosti týkající se systému EKIS jsou uživatelé povinni provádět v souladu s obecně závaznými právními předpisy a interními akty řízení.
6) Jakoukoliv změnu v připojení pracovní stanice do systému EKIS (případně jejího nastavení) může provést pouze administrátor (na základě doporučení odborného útvaru nájemce).

7) Každá pracovní stanice, ze které se přistupuje do systému EKIS (SAPGUI, WEB aplikace) musí mít instalován antivirový programu, který je pravidelně aktualizován. Instalaci a údržbu provádí administrátor koncové stanice. Uživatel nesmí svévolně do této instalace zasahovat.
8) Na pracovních stanicích systému EKIS se smí používat pouze software licencovaný MV a schválený řídící radou projektu (např. kancelářský software, resp. MS Office).
9) Je povinností dodržovat preventivní opatření doporučená k ochraně před počítačovými viry.
10) Bezpečnostní opatření:
    a) informační systém EKIS není certifikován podle zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti musí však splňovat podmínky zákona č. 101/2000 Sb., o ochraně osobních údajů a porušení bezpečnostních pravidel může být řešeno ve smyslu zákona č. 40/2009 Sb., trestní zákoník - § 230 – 232.
    b) informace o postupu přihlášení do systému EKIS, tzn.: údaje o ID uživatele a používaných heslech, nesmí být v žádné formě zapisovány do kalendářů, diářů, souborů na PC, poznámek na stole atd.;
    c) všechna externí magnetická média obsahující citlivé informace, musí být uschovávána na zabezpečeném místě a zajištěna před neautorizovaným přístupem.V případě likvidace dat na těchto médiích musí být použita technologie bezpečného výmazu dat popř. likvidace médií;
    d) s nosiči informací (např. tiskové výstupy, magnetická a optická záznamová média) obsahující osobní údaje dle zákona č. 101/2000 Sb., o ochraně osobních údajů, musí být nakládáno v souladu s tímto zákonem a s NMV č. 5/2008, kterým se vydává spisový a skartační řád MV;
    e) s nosiči informací (např. tiskové výstupy, magnetická a optická záznamová média) obsahující citlivé údaje vyexportované ze systému EKIS s NMV č. 5/2008, kterým se vydává spisový a skartační řád MV;
    f) všechny zastaralé a/nebo nepoužitelné materiály, obsahující citlivé informace, musí být bezpečně zlikvidovány v souladu s platnými předpisy o likvidaci materiálů obsahujících citlivé informace;
    g) pokud je uživateli přiděleno více autorizací (např. autorizace administrátora a autorizace uživatele), musí být použita vyšší autorizace pouze na nezbytně nutnou dobu potřebnou pro činnosti vyžadující vyšší autorizaci.
    h) pracovní stanice musí být zajištěny před neautorizovaným užitím (zavedením přístupového hesla při spuštění počítače, spořiče obrazovky chráněné heslem s intervalem spuštění max. 5 minut, aj.);

Svým podpisem stvrzuji, že jsem byl/a poučen/a o bezpečnosti a ochraně dat v systému EKIS.

Jméno pracovníka / OEČ: ……. Školení provedl: ……..
Podpis / datum: …… ……..Podpis / datum: ……
Výtisk č. 1 obdrží pracovník
Výtisk č. 2 založit do personálního spisu
Výtisk č. 3 přiložit k žádosti o zřízení oprávnění přístupu do systému EKIS
Převzal dne: …….. Podpis pracovníka: ……
Poznámky: ……

PŘÍLOHA P IV: ŽÁDOST O ZŘÍZENÍ OPRÁVNĚNÍ PŘÍSTUPU DO SYSTÉMU EKIS PRO UŽIVATELE

Žádost o zřízení oprávnění přístupu do systému EKIS pro uživatele

(žádost pro uživatele, který požaduje přístup na více než vlastní personální oblast)

Uživatel zaveden v produktivním systému: EKIS I. ☐ ***Od:*** ***EKIS II. Od:*** ☐

Příjmení:	*Jméno:*	*Titul:*
Osobní evidenční číslo:	*Služební telefon:*	
Odbor/Oddělení:	*Funkce:*	
Úplný název útvaru:	*Dislokace útvaru:*	
Číslo účetního okruhu:	*Číslo zúčtovací oblasti:*	
Personální pravomoc:	*Kázeňská pravomoc:*	
Zpřístupnění pro čtení:	*Označení referenta v systému:*	
Číslo vlastní personální oblasti:	*Číslo vlastních dílčích personálních oblastí:*	
****) Čísla požadovaných personálních oblastí:***	****) Čísla požadovaných dílčích personálních oblastí:***	

**1 Označení referenta je nutné pro zasílání interní pošty v systému (bližší informace školitel) ZKRATKA V SYSTÉMU SAP*

Záznamy o školeních uživatele ***(uvádějte prosím do názvu školení níže uvedené zkratky)***

Název a obsah školení koncového uživatele (označení modulu)	*Délka školení*	*datum*	*Příjmení Lektora*	*podpis lektora*	*podpis uživatele*	*poznámka*
Bezpečnostní školení. Základní bezpečnostní směrnice, pravidla, ***uzavření dohody o mlčenlivosti***. **(Povinné pro všechny uživatele!)**	1 hod.					
Vstupní školení (ovládání systému)	1 den					

Role uživatele v informačním systému EKIS

Technický název	**Název uživatelské role**

Rozsah přístupových oprávnění

☐ **systém HR3** ☐ **systém MV3** ☐ **WEB** ☐

Workplace

Upřesnění oprávnění: (Finanční místa, Rozpočtové položky, Nákladová střediska / uzel nákl. stř., Materiálová třída, Druhy pohybu, Sklady,…..

Schvalovací doložka

Vyplní žadatel a příslušní funkcionáři

Podpis uživatele: ……..... v ..... dne .....

Doložka žadatele - vlastníka primárních dat (ředitel útvaru s personální pravomocí)

Svým podpisem stvrzuji, že:

- **požadavek o přidělení oprávnění přístupu výše uvedenému uživateli pro autorizovaný přístup do systému EKIS, který je zřizován v souladu s pracovní náplní uživatele,**
- **pominou-li důvody přístupu do systému EKIS dle navrhované autorizace pro tohoto uživatele, oznámím písemně tuto skutečnost kompetenčnímu středisku EKIS (OIEP MV),**
- **uživatel absolvoval bezpečnostní školení a byl poučen o povinnostech vyplývajících ze zákona 101/2000 Sb. O ochraně osobních údajů a oba tyto záznamy řádně podepsané uživatelem jsou uloženy v jeho personálním spisu.**

Funkce žadatele**:** ……..... Příjmení / jméno: .....

Podpis žadatele: ..... v ..... dne .....

Zdůvodnění žádosti:

……

……..

*) **Doložka správce dat – vlastníka sekundárních dat::** **EKIS I** ředitel odboru účetnictví a statistiky MV ČR
EKIS II ředitel odboru personálního MV ČR

Svým podpisem akceptuji požadavek zařazení výše uvedeného uživatele do systému EKIS v souladu s výše schválenými rolemi a autorizací.

Podpis správce dat EKIS I..... v ..... dne .....

Podpis správce dat EKIS II..... v ..... dne .....

Záznamy administrátora

Do systému zavedl: ……..... dne .....

Ze systému vyřadil: ……..... dne .....

Poznámky:

Označení pro finanční a materiálové moduly: *finanční účetnictví **FI,** rozpočet **TR**, investiční majetek **AM**, hospodářství **MM**, drobný dlouhodobý majetek **DDM**, nákladové účetnictví **CO**, Pokladní kniha SAP R/3 **PoK** , Peněžního deník Lotus Notes **PeD;.***

Označení pro moduly HR: *vzdělávání **VZ**, organizační management **OM**, nábor a výběr **NaV**, personální administrace **PA**, odměňování **MU,** soc. zabezpečení **SE** , **WEB**, manažerský inf.systém **MIS**, portál – Workplace **WP**, materiálové zabezpečení - oděvní výdejny **OV.***

Inicializační heslo: ……

PŘÍLOHA P V: ŽÁDOST O ZMĚNU NEBO DOPLNĚNÍ OPRÁVNĚNÍ PŘÍSTUPU DO SYSTÉMU EKIS PRO UŽIVATELE

Žádost o změnu nebo doplnění oprávnění přístupu do systému EKIS pro uživatele

Uživatel zaveden v produktivním systému: EKIS I. ☐ ***:*** ***EKIS II.*** ***Od*** ☐

Příjmení:	*Jméno:*	*Titul:*
Osobní evidenční číslo:	*Služební telefon:*	
Odbor/Oddělení:	*Funkce:*	
Úplný název útvaru:	*Dislokace útvaru:*	
Číslo účetního okruhu:	*Číslo personální oblast:*	
Číslo zúčtovací oblasti:	*Číslo dílčí personální oblast:*	
Personální pravomoc:	*Kázeňská pravomoc:*	
Zpřístupnění pro čtení:	*Označení referenta v systému(*1)*	

**1 Označení referenta je nutné pro zasílání interní pošty v systému (bližší informace školitel) ZKRATKA V SYSTÉMU SAP*

Záznamy o školeních uživatele ***(uvádějte prosím do názvu školení níže uvedené zkratky)***

Název a obsah školení koncového uživatele (označení modulu)	*Délka školení*	*datum*	*Příjmení Lektora*	*podpis lektora*	*podpis uživatele*	*poznámka*
Bezpečnostní školení. Základní bezpečnostní směrnice, pravidla, ***uzavření dohody o mlčenlivosti***. (**Povinné pro všechny uživatele!)**	1 hod.					
Vstupní školení (ovládání systému)	1 den					

Role uživatele v informačním systému EKIS

Technický název	**Název uživatelské role**

Rozsah přístupových oprávnění

☐ **školní klient MV2**	☐ **produkční klient MV3**	☐ **LN**	☐ **MV1 –**
☐ **školní klient HR2**	☐ **produkční klient HR3**	☐ **WEB**	☐ **Workplace**

Upřesnění oprávnění: (Finanční místa, Rozpočtové položky, Nákladová střediska / uzel nákl. stř., Materiálová třída, Druhy pohybu, Sklady,.....)

Schvalovací doložka

Vyplní žadatel a příslušní funkcionáři

Podpis uživatele: ……..... v ..... dne .....

Doložka žadatele.
Svým podpisem stvrzuji požadavek o přidělení oprávnění přístupu výše uvedenému uživateli pro autorizovaný přístup do systému EKIS, který je zřizován v souladu s pracovní náplní uživatele. Zároveň stvrzuji, že pominou-li důvody přístupu do systému EKIS dle navrhované autorizace pro tohoto uživatele, oznámím písemně tuto skutečnost "vlastníku" a správci systému EKIS.

Funkce žadatele**:** ……..... Příjmení / jméno: .....

Podpis žadatele: ..... v ..... dne .....

Doložka správce systému.
Svým podpisem akceptuji požadavek zařazení výše uvedeného uživatele do systému EKIS v souladu s výše schválenými rolemi a autorizací.

Funkce správce systému:…….. Příjmení / jméno: .....

Podpis: ..... v ..... dne .....

Záznamy administrátora

Do systému zavedl: .....……..... dne .....

Ze systému vyřadil: .....……..... dne .....

Poznámky:

Označení pro finanční a materiálové moduly: *finanční účetnictví **FI,** rozpočet **TR**, investiční majetek **AM**, hospodářství **MM**, drobný dlouhodobý majetek **DDM**, nákladové účetnictví **CO**, Pokladní kniha SAP R/3 **PoK** , Peněžního deník Lotus Notes **PeD;.***

Označení pro moduly HR: *vzdělávání **VZ**, organizační management **OM**, nábor a výběr **NaV**, personální administrace **PA**, odměňování **MU,** soc. zabezpečení **SE** , **WEB**, manažerský inf.systém **MIS**, portál – Workplace **WP**, materiálové zabezpečení - oděvní výdejny **OV.***

Inicializační heslo: ……..

PŘÍLOHA PV I: ŽÁDOST O ZRUŠENÍ OPRÁVNĚNÍ PŘÍSTUPU DO SYSTÉMU EKIS

Žádost o zrušení oprávnění přístupu do systému EKIS

Žádáme o zrušení oprávnění přístupu do systému EKIS pro níže uvedeného uživatele:

Útvar (org. jednotka): ……..…….....……..……..

Účetní okruh, pers. oblast, zúčtovací okruh (1*):……

Příjmení, jméno uživatele: ……OEČ (funkce): ……Ke dni:……

Požadavek na zrušení oprávnění v systému EKIS (1*) :

• školní klient MV2 • produkční klient MV3 • LN • MV1 – pouze členové RT

• školní klient HR2 • produkční klient HR3 • WEB • – Workplace

Funkce žadatele:……..... Příjmení žadatele: .....

Svým podpisem stvrzuji požadavek o zrušení oprávnění přístupu výše uvedeným uživatelům pro autorizovaný přístup do systému EKIS
v souladu s pracovní náplní uživatele.

Podpis žadatele : ..... v ..... dne .....

Funkce "vlastníka": ..... Příjmení "vlastníka": .....

Svým podpisem akceptuji požadavek vyřazení výše uvedených uživatelů ze systému EKIS .

Podpis "vlastníka" :…. .....v ..... dne .....

Záznamy administrátora:

Výmaz ze systému provedl :…. ..... dne .....

Poz. (1*). nehodící se škrtněte.