Personální informační systém Policie ČR při mimořádných událostech

Bc. Jiří Minichbauer

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jiří MINICHBAUER**
Studijní program:	**N 2808 Chemie a technologie materiálů**
Studijní obor:	**Řízení technologických rizik**
Téma práce:	**Personální informační systém Policie ČR při mimořádných událostech.**

Zásady pro vypracování:

1. **Cílem diplomové práce je popis činností vedoucí ke zmírnění negativních dopadů v důsledku nefunkčnosti personálního informačního systému při řízení policejních akcí.**
2. **Provést analýzu rizik, vytipovat zranitelná místa a navrhnout protiopatření ke snížení rizik.**
3. **V praktické části rozpracovat prvky řešení mimořádných událostí v aplikaci personálního informačního systému Policie ČR.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] DOBDA, L. Ochrana dat v informačních systémech.Praha: Grada, 1998. ISBN 80-7169-479-7

[2] POŽÁR, L. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk,s.r.o., 2005. ISBN 80-86898-38-5

[3] VALÁŠEK J., KOVAŘÍK F. a kolektiv, Krizové řízení při nevojenských krizových situacích, Ministerstvo vnitra – generální ředitelství HZS ČR, 2008. ISBN 987-80-86640-93-8

[4] Zákon č. 273/2008 Sb. ze dne 17. července 2008 o Policii České republiky

[5] Zákon č. 361/2003 Sb. ze dne 23. září 2003 o služebním poměru příslušníků bezpečnostních sborů

Vedoucí diplomové práce: **RNDr. Jaroslav Tupý**
Ústav krizového řízení

Datum zadání diplomové práce: **12. února 2010**

Termín odevzdání diplomové práce: **23. dubna 2010**

V Uherském Hradišti dne 17. února 2010

L.S.

Ing. Vladimír Mrkvička, Ph.D.
děkan

RNDr. Jaroslav Tupý
ředitel ústavu

ABSTRAKT

Cílem této práce je vytvořit popis činností vedoucí ke zmírnění negativních dopadů v důsledku nefunkčnosti personálního informačního systému Policie ČR při řízení policejních akcí. Teoretická část popisuje ekonomický informační systém Ministerstva vnitra, jehož součástí je personální informační systém policie. Vysvětluje funkci personálního systému Policie. V praktické části je provedena ukázková analýza rizik s vytipováním zranitelných míst a s návrhem protiopatření ke snížení rizik. Autor předpokládá využití této práce jako podklad při vypracování krizových plánů pro provoz personálního informačního systému policie a Ministerstva vnitra.

K vypracování diplomové práce byla využita odborná literatura vztahující se k dané problematice.

Klíčová slova:

fyzická bezpečnost, personální bezpečnost, režimová bezpečnost, technická bezpečnost, programová bezpečnost, datová bezpečnost, komunikační bezpečnost, architektura systému, riziko, aktiva, analýza rizik

ABSTRACT

The aim of this work is to create a description of activities to mitigate the negative impacts due to malfunction of personal information system of the police of the Czech Republic in the management of police actions. The theoretical part describes the economic information system of the Ministry of Interior, which includes police personnel information system. It explains the function of the police personnel system. The practical part includes an exemplary risk analysis with suggestion of vulnerabilities and proposed countermeasures to reduce risks. The author assumes the use of this work as a basis for drawing up emergency plans for operating police personnel information system and the Ministry of Interior.

For the development of this thesis the literature related to the topic was used.

Keywords:

physical security, personal security, procedural security, technical safety, program secutity, data security, communications security, system architecture, risk, assests, risk analysis,

Tímto děkuji vedoucímu své bakalářské práce, panu RNDr. Jaroslavu Tupému, za vedení, cenné rady a podnětné připomínky při tvorbě této práce, pracovníkům Policejního prezidia ČR, jmenovitě řediteli plk. Ing. Romanu Fidlerovi Ředitelství pro řízení lidských zdrojů PP ČR a vedoucímu oddělení krizového řízení PP ČR plk. Ing. Milanu Fialovi. Dále pracovníkům Ministerstva vnitra spravující systém EKIS a pracující ve funkcích manažera nastavení, kteří mi poskytli mnoho důležitých informací.

Motto: Nám se to rozhodně nemůže stát!

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v archivu Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou 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 práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové 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 práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti dne 19. dubna 2010

…….……
podpis studenta/ky

OBSAH

ÚVOD

Tato diplomová práce se zabývá personálním informačním systémem Policie České republiky jeho potřebou při mimořádných situacích. K výběru tématu mé diplomové práce z oblasti bezpečnosti informačních systémů jsem se rozhodl, protože se této problematice věnuji více než deset let na Ministerstvu vnitra České republiky. Poslední dobou se zabývám bezpečností ekonomického informačního systému Ministerstva vnitra (dále jen EKIS), jehož nedílnou součástí je personální informační systém Policie České republiky nazvaný EKIS II. Smyslem této diplomové práce je popsání jeho základní funkcionality systému a jeho implementaci v prostředí Policie ČR na základě zákonných norem.
V práci se chci věnovat hlavně zabezpečení systému z pohledu objektové bezpečnosti, výběr vhodných lokalit pro umístění koncových pracovišť IS, vybudování náhradních řešení použitelných při mimořádné situaci. Vytipovat zranitelná místa systému, provést analýzu hrozeb, ocenění rizik a navrhnout opatření zmírňujících následky při mimořádných situacích.

I TEORETICKÁ ČÁST

1 PERSONÁLNÍ EVIDENCE

Personální evidence se řídi zákonem č. 361/2003 Sb. ze dne 23. září 2003 o služebním poměru příslušníků bezpečnostních sborů, ve znění pozdějších předpisů, nařízením Ministerstva vnitra č. 20/2007 ze dne 14. února 2007 o personální evidenci a o zpracovávání osobních údajů, které s ní souvisejí.

Personální evidencí se rozumí soubor osobních údajů vedený v rozsahu stanoveném ve výše uvedených zákonných předpisech. Při vedení tohoto souboru se postupuje podle zvláštního právního předpisu.

Personální evidence jsou vedeny Personálním pracovištěm příslušného útvaru, popřípadě jiným pracovištěm na základě organizačního řádu příslušného útvaru[1] a jsou vedeny v souladu s Nařízením Ministerstva vnitra č. 20/2007:

- elektronicky čl. 6 a čl. 7. automatizované zpracování personálních dat v ekonomickém informačním systému ministerstva vnitra EKIS II. formou evidenčních dokladů, popřípadě v modulu WEB, který je jeho součástí
- v listinné podobě čl. 17 a čl. 18 listinné zpracování personálních dat formou Osobního spisu příslušníka nebo zaměstnance.

Pro plnění úkolů Policie ČR a Ministerstva vnitra se ze systému EKIS II poskytují data oprávněným útvarům resortu MV a případným dalším oprávněným žadatelům:
oddělení personální bezpečnosti a lustrací bezpečnostního odboru MV, integrovanému operačnímu středisku Policejního prezidia ČR, orgánům činných v trestním řízení, vedoucím zaměstnancům s personální pravomocí, přímým nadřízeným, velitelům služeb aj.

Z výše uvedeného vyplývá, že převážná část personální evidence je vedena v elektronické podobě a při výpadku personálního informačního systému by nebylo možné při celkovém množství policistů vést náhradní evidenci. Nehledě k tomu, že pří vedení náhradní evidence by mohlo dojít k nekonzistenci dat v náhradních dokladech a v personální evidenci.

Veškerá data o průběhu služebního poměru slouží po jeho ukončení k výměře výsluhového příspěvku příslušníka a další finanční náležitosti.

[1] Čl. 20 nařízení Ministerstva vnitra č. 51/2006

1.1 Plánování služeb

Nezbytnou součástí personálního systému plánování služeb, které je realizováno aplikací WEB v LOTUS NOTES v souladu se zákonem č. 361/2007 Sb. § 53 odst. 1, ze kterého vyplývá povinnost plánovat dobu služby předem, a to zpravidla na období 1 měsíce. Změna rozvržení doby služby musí být oznámena příslušníkovi zpravidla nejpozději 3 dny před nástupem do služby nejpozději však 1 den předem počátek směny.

Personální informační systém podléhá zákonu č. 101/2000 Sb. ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů. Dále se řídí „Bezpečnostní politikou Ministerstva vnitra v oblasti informačních systémů“ a resortní předpisy Ministerstva vnitra.

1.2 Požadavky na dostupnost informačního systému

Na základě výše uvedených právních předpisů a povaze zpracovávaných informací je definována doba a způsob zpřístupnění personálního systému způsobem:

- zpřístupnění pro zadávání nových a aktualizace již existujících informací pondělí až pátek 6.30 – 18.00 hod
- zpřístupnění pro vytěžování vybraných informací nepřetržitě
  po celý týden 24 hod. denně

1.3 Data a je jich pohyb v personální evidenci

V systému EKIS II. je vedena personální agenda Policie České republiky, která obsahuje 43 538 záznamů o policistech a 10 648 záznamů o občanských zaměstnancích.

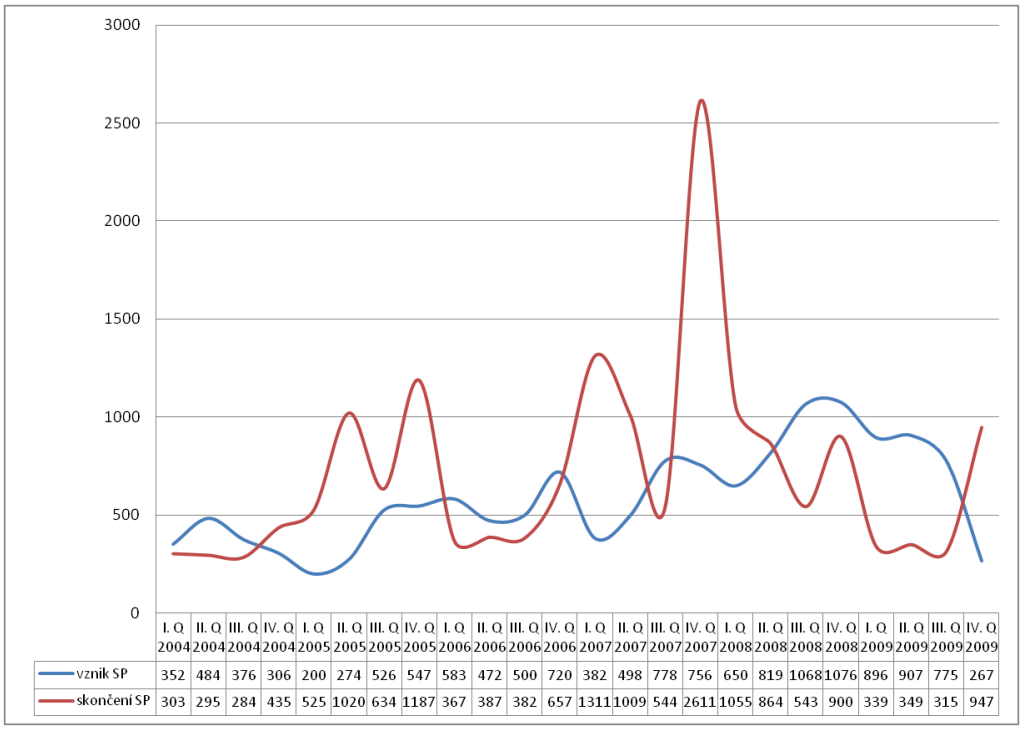
Policisté	43538
Občanští zaměstnanci	10648
Celkem	***54186***

Tabulka 1 - Počty pracovníků Policie ČR

Celkové počty pracovníků nemají vypovídající schopnost o využitelnosti a důležitosti systému EKIS II. pro prácí personálních pracovišť a pro řízení Policie ČR. Je důležité uvést další statistické údaje:

- přehled počtu skončení a vzniku služebního poměru po čtvrtletích za období 2004-2009 (nejsou zde uvedeny přesuny policistů mezi jednotlivými útvary)
- počet změn systemizace v letech 2002 - 2009
  dopady realizovaných změn v systemizaci na počty pracovních míst

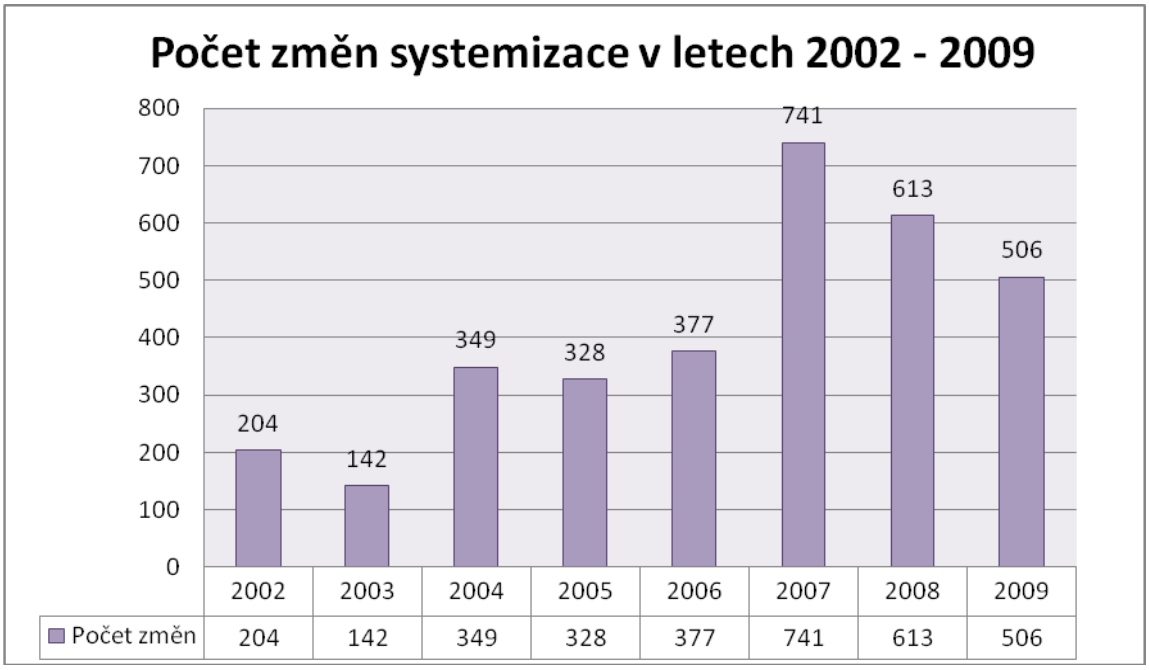
V tabulce a grafu počtu změn systemizace je uveden přehled změn v systemizaci. Všechny tyto změny mají dopad na velký počet policistů, pro které je potřeba následně vygenerovat personální opatření.



	I. Q 2004	II. Q 2004	III. Q 2004	IV. Q 2004	I. Q 2005	II. Q 2005	III. Q 2005	IV. Q 2005	I. Q 2006	II. Q 2006	III. Q 2006	IV. Q 2006	I. Q 2007	II. Q 2007	III. Q 2007	IV. Q 2007	I. Q 2008	II. Q 2008	III. Q 2008	IV. Q 2008	I. Q 2009	II. Q 2009	III. Q 2009	IV. Q 2009
vznik SP	352	484	376	306	200	274	526	547	583	472	500	720	382	498	778	756	650	819	1068	1076	896	907	775	267
skončení SP	303	295	284	435	525	1020	634	1187	367	387	382	657	1311	1009	544	2611	1055	864	543	900	339	349	315	947

Tabulka 2 - Skončení a vznik služebního poměru (

Příloha 1.)



Tabulka 3 - Počty změn systemizace v letech 2002 - 2009

Rok	Počet změn	Duvod změny	Dopad na pracovní místa
2006	377		redefinice všech služebních míst 47000
2007	741	účinnost služebního zákona	přesuny okresních ředitelství policie - redefinice všech 58000 míst
2008	613	reforma policie I	zřízení krajských ředitelství policie - redefinice všech 58000 míst
2009	506	reforma policie II	zřízení 6 nových KŘP - redefinice cca 35000 míst

Tabulka 4 - Dopady realizovaných změn v systemizaci na počty pracovních míst

2 EKIS II.

Ekonomický informační systém resortu[2] Ministerstva vnitra EKIS je vybudován jako centrální systém. Je rozdělen podle charakteru zpracovávaných dat a podle doby implementace na dvě části - EKIS I a EKIS II.

- Část EKIS I je určena pro zpracovávání finančního účetnictví, materiálových evidencí (tato část není předmětem této práce),
- Část EKIS II je určena pro personální evidence, systemizaci[3] a vzdělávání a zpracování mezd a platů zaměstnanců resortu Ministerstva vnitra.

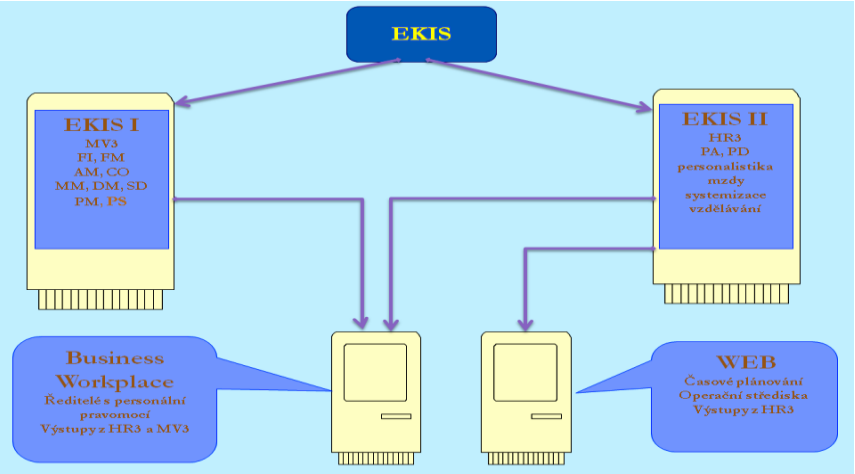
Základ systému tvoří softwarový produkt Systém R/3 od firmy SAP s podpůrnými subsystémy LOTUS DOMINO obsahující WEB aplikaci a manažerský informační systém SAP Business Workplace umožňující provádění analýz v ekonomické oblasti, personalistice, systemizaci a ve vzdělávání.

Hardware i software je v pronájmu od firmy IBM Česká republika, spol. s r.o. a je umístěn ve výpočetním středisku Ministerstva vnitra. Odpovědnost za funkčnost centrální části systému má pronajímatel, který je zároveň garantem nastavení systému podle podkladů dodaných Ministerstvem vnitra. Ministerstvo vnitra zabezpečuje přístup k systému EKIS prostřednictvím sítě WAN (intranet Ministerstva vnitra) zodpovídá za funkčnost této sítě. Všechna pracoviště využívající EKIS mají přístup do systému zabezpečen těmito sítěmi.

Jako pracovní stanice jsou využity běžné kancelářské počítače propojené prostřednictvím sítě intranet do centrální části sytému. Vzhledem k tomu, že se jedná o centrální systém, mohou uživatelé do tohoto systému přistupovat na svůj účet z jakéhokoliv počítače připojeného v síti intranet ministerstva vnitra.

[2] Resort ministerstva vnitra zahrnuje Úřad ministerstva vnitra (vlastní ministerstvo), Policii ČR, Hasičský záchranný sbor a samostatné organizační složky státu zřízené ministerstvem vnitra

[3] Systemizací se rozumí stanovení počtu služebních míst včetně počtu míst příslušníků zařazených v zálohách a objemu prostředků stanovených státním rozpočtem na příslušný rok na jejich služební příjmy



Obrázek 1- Schéma ekonomického informačního systému EKIS

2.1 Přístupy do systému

2.1.1 Způsob přístupu do systému EKIS II.

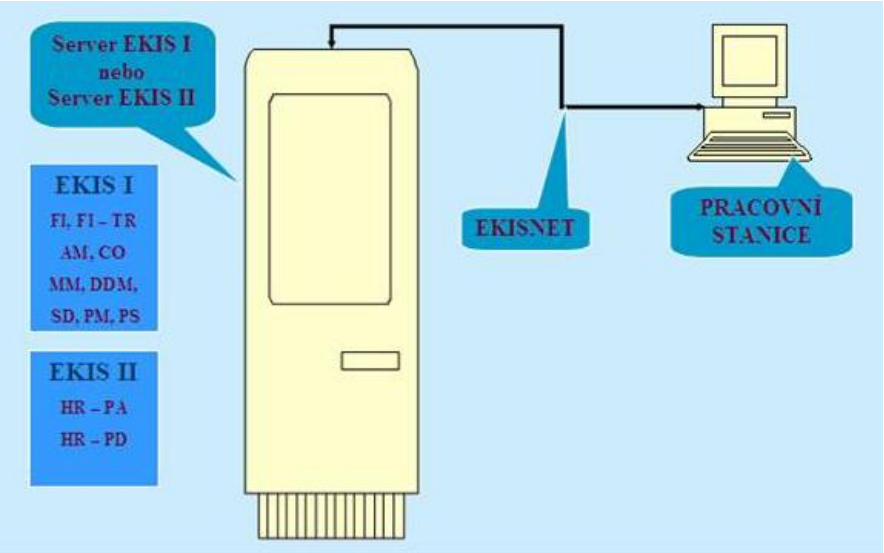
Přístup do systému EKIS II. je zprostředkován třemi způsoby:

- Přímý přístup do R/3 prostřednictvím klienta SAP GUI
- Přístup do systému je zprostředkovaný WEB aplikací LOTUS DOMINO
- Přímý přístup serverem do R/3 prostřednictvím Business Workplace

2.1.1.1 Přímý přístup prostřednictvím klienta SAP GUI

Na pracovní stanici SAP GUI realizuje tzv. prezentační část architektury, obrazuje data ze serveru a zprostředkovává jejich vstup. Na klientské stanici se neukládají žádná data, jsou zde uloženy pouze soubory reprezentující SAP GUI.

SAP GUI prostřednictvím sítě resortu Ministerstva vnitra komunikuje TCP/IP protokolem s aplikačním serverem. Předpokládá se přímé spojení mezi pracovní stanicí a aplikačním serverem. Aplikační servery přistupují pomocí sítě LAN k jednomu databázovému serveru, na kterém jsou uložena veškerá data aplikace.



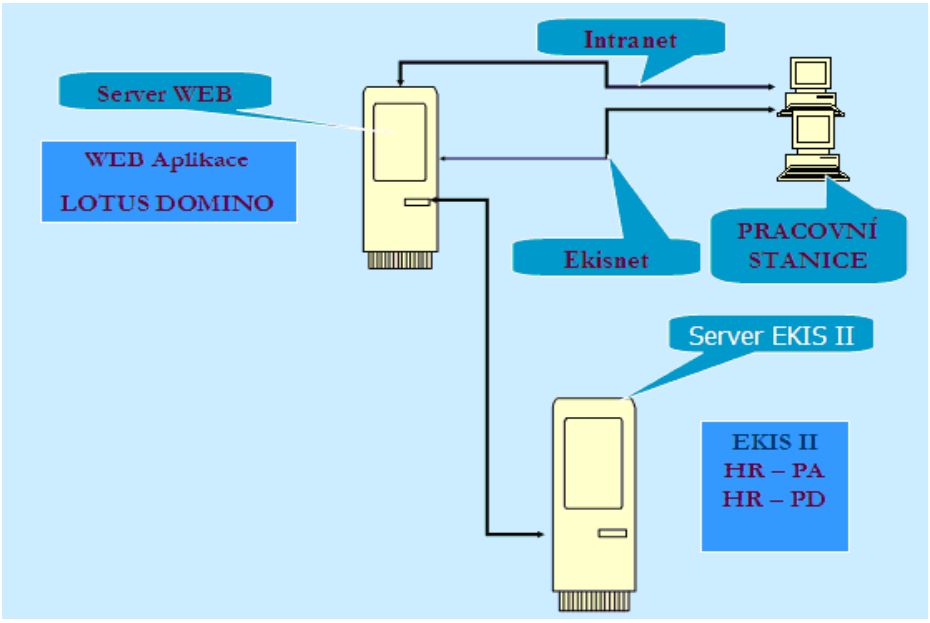
Obrázek 2 - Přístup prostřednictvím klienta SAP GUI

2.1.1.2 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.

Rozdíly proti přístupu přes SAP GUI:

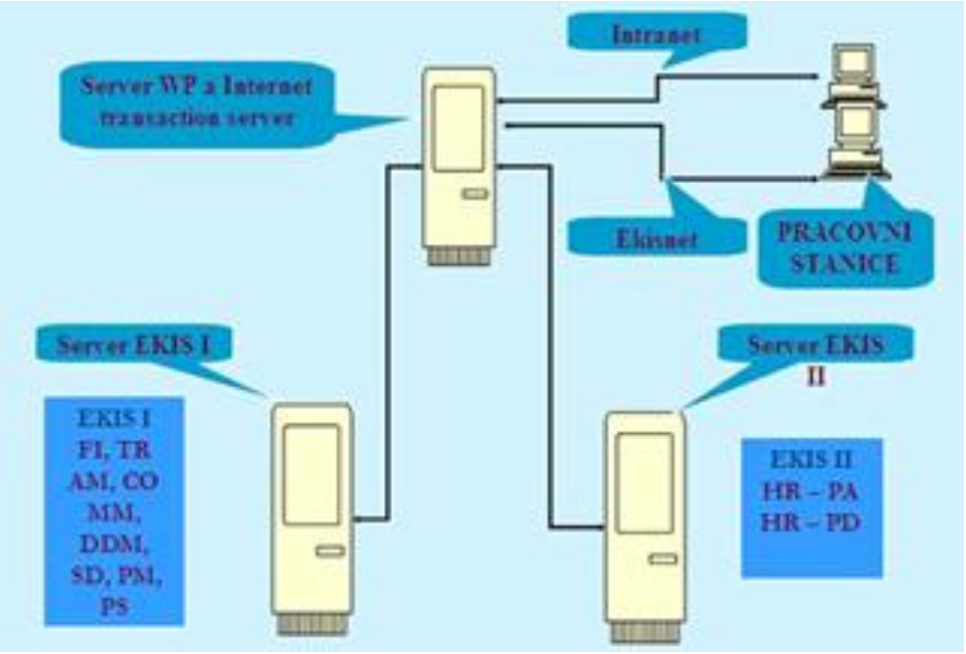
- aplikace je provozována off-line
- její funkce nejsou bezprostředně závislé na dostupnosti serveru/sítě
- data jsou ukládána lokálně a následně jsou replikována do centrálního serveru LOTUS DOMINO, který zprostředkovává automatické zaúčtování do systému R/3.



Obrázek 3 - Zprostředkovaný přístup WEB aplikací

2.1.1.3 Přístup pomocí aplikace SAP Business Workplace

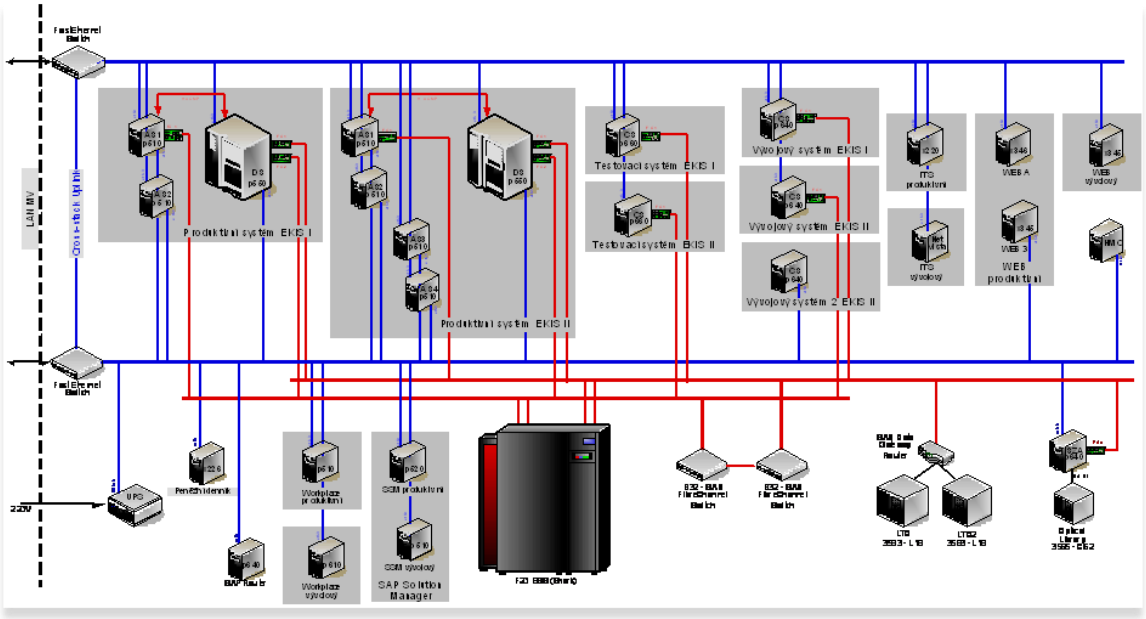
Uživatelská stanice není vybavena žádným klientem, uživatel přistupuje do systému prostřednictvím webovského prohlížeče Microsoft Explorer. Uživatelské rozhraní SAP Business Workplace nepřistupuje do systému SAP R/3 přímo a data pro něho transformuje „SAP Internet transaction server“, který zabezpečuje přístup k datům. Přístup uživatelů jednotlivých systémů R/3 se děje automaticky bez vědomí uživatelů je zajištěn metodou Single Sign-on . Přístup do systému je zprostředkován resortními sítěmi INTRANET nebo EKISNET.



Obrázek 4 - Uživatelské rozhraní SAP Business Workplace

2.2 Architektura systému EKIS

EKIS je vybudován jako centrální systém s jedním serverovým pracovištěm. Na tomto pracovišti jsou nainstalována všechna technologická zařízení centrální části



Obrázek 5 - Architektura centrální části (Příloha 2)

V současné době provoz systému zajišťuje 27 serverů[4], které zabezpečují provoz celého systému. Všechny systémy centrální části ukládají svá data na externí diskové pole. Lokální disky slouží pouze pro operační systém jednotlivých serverů, systémové programy a swap soubory.

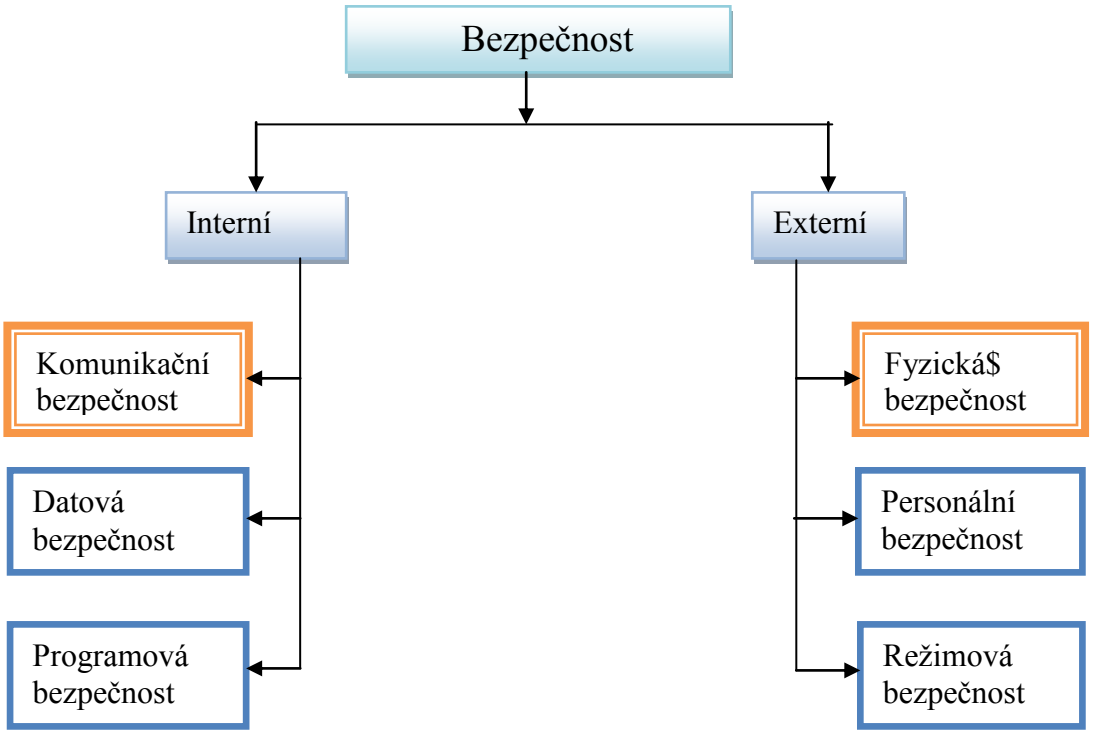
Na serverech je instalován operační systém AIX (UNIX IBM). Data se ukládají do databáze ORACLE, která je spolu se softwarový produktem Systém R/3 Enterprise od firmy SAP základem systému EKIS. WEB aplikace je implementována v prostředí Lotus Domino. Pro archivaci je použit archivační software Common Store.

[4] Na základě smluvního závazku mezi IBM s.r.o. a MV ČR nelze konfiguraci serverů zveřejnit

3 BEZPEČNOST SYSTÉMU EKIS

Bezpečnost informačního systému tvoří soubor opatření z oblasti:

- počítačové a komunikační bezpečnosti,
- administrativní bezpečnosti a organizačních opatření,
- personální bezpečnosti,
- fyzické bezpečnosti informačního systému.



- Komunikační bezpečnost – řeší problematiku ochrany komunikací mezi jednotlivými komponentami informačního systému a definuje způsob zajištění integrity přenášených dat po komunikačních cestách (LAN, WAN).
- Datová bezpečnost – zahrnuje ochranu dat v souborech a databázích proti neoprávněné změně, poškození nebo ztrátě.
- Programová bezpečnost – bezpečnost programového vybavení, především operačních systémů, řízení databází a aplikačních programů
- Fyzická bezpečnost IS – se zabývá zabezpečením budov, ve kterých je IS umístěn. Ochranou těchto budov před přírodními vlivy, požárem a opatřeními před neoprávněným vniknutím osob do objektů. Dále sem patří provoz a údržba technologických vybavení budov (stabilizovaná dodávka el. energie, klimatizace aj.)

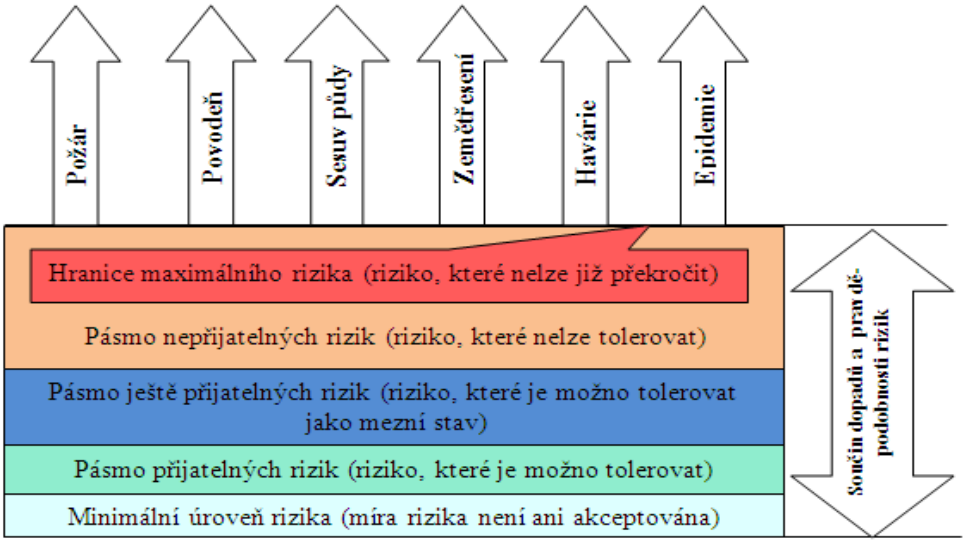
- Personální bezpečnost – zabývá se eliminací hrozeb způsobených lidským faktorem. Ochranou IS před nedovoleným jednáním pracovníků. Určuje, která potřebná školení musí uživatel absolvovat pro svoji práci.
- Režimová bezpečnost – zabývá se právními normami a bezpečnostními předpisy.

3.1 Hrozba

Hrozba je skutečnost , událost, síla nebo osoby jejichž působení nebo činnost mohou způsobit poškození, zničení, ztrátu důvěry nebo hodnotu aktiva. Hrozba může ohrozit bezpečnost jakéhokoliv systému. Soupis vybraných hrozeb je v tabulce Přehled vybraných hrozeb.

3.2 Riziko

Riziko je chápáno jako potenciální nebezpečí, že daná hrozba využije zranitelnosti systému, tak aby způsobila ztrátu nebo poškození aktiv nebo skupiny aktiv. Dále je charakterizováno jako kombinace dvou faktorů, pravděpodobností výskytu nežádoucí hrozby. Negativní dopady mohou vyvolat ztráty na životech nebo zdraví osob, na majetku a narušení životního prostředí. Riziko je spjato s místem a časem působení jeho příčin.

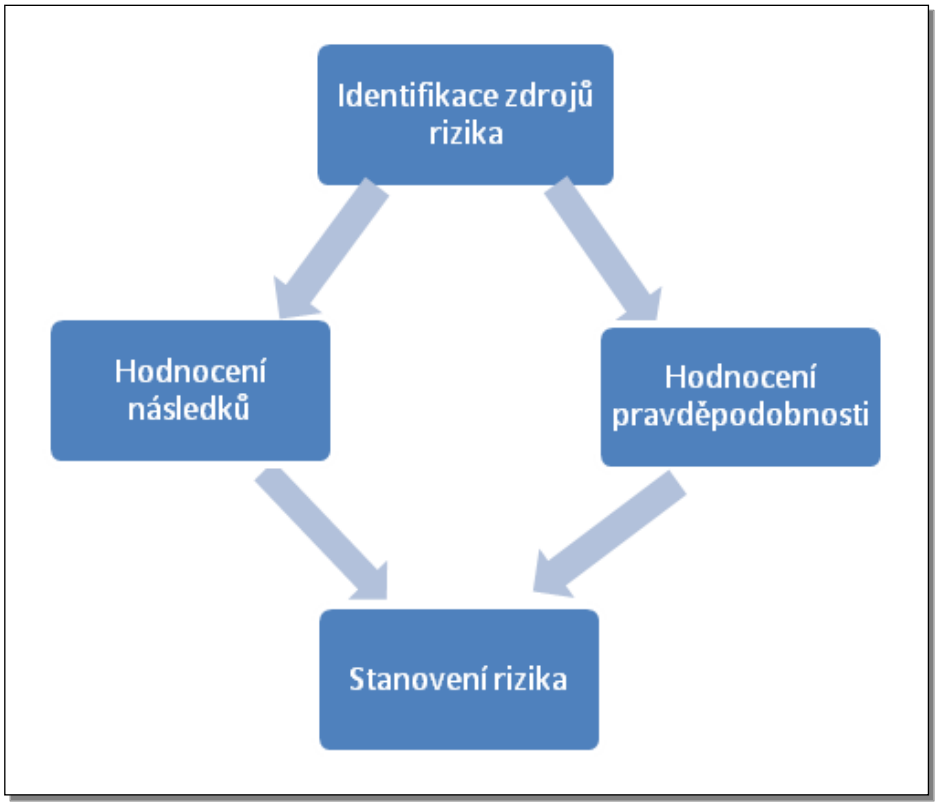


Obrázek 6 - Riziko a jeho akceptovatelnost

Každý člověk vnímá a hodnotí riziko specifickým způsobem. Jinými slovy je to vztah mezi člověkem a jeho okolím. Úroveň rizika je možno seřadit podle akceptovatelnosti. Projevené riziko může svými dopady vyvolávat příčiny ke vzniku nových rizik k tzv. dominoefekt.

3.3 Analýza rizik

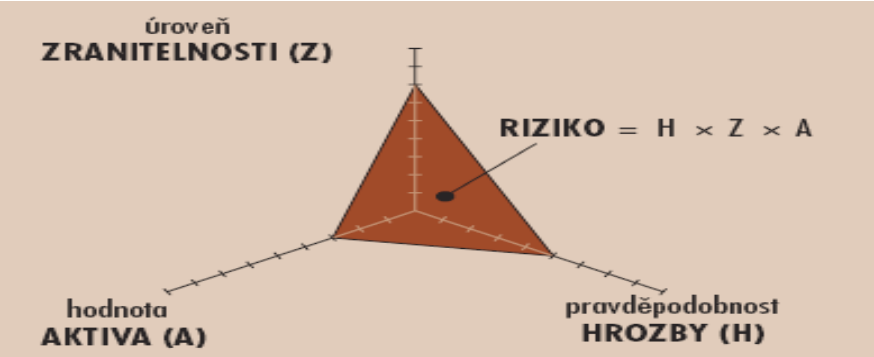
Analýza rizik (riziková analýza) – je proces, který identifikuje a klasifikuje informační aktiva společnosti (organizace), odhaluje hrozby, stanovuje rizika a navrhuje bezpečnostní opatření. Aktivy jsou zejména informace a data, která firma zpracovává. Nezáleží na tom, zda jsou informace v elektronické či papírové podobě.



Obrázek 7 - Základní kroky analýzy rizik

Analýza rizik zpravidla zahrnuje následující kroky.

- Identifikace aktiv a požadavků na jejich ochranu – klasifikace informací.
- Analýza hrozeb a zranitelností.
- Stanovení míry rizika vztahující se k jednotlivým aktivům.
- Návrh bezpečnostních opatření ke snížení rizika na akceptovatelnou úroveň.



Obrázek 8 - Zranitelnost

Výsledky analýzy rizik musí být objektivním podkladovým materiálem pro rozhodování o dalším postupu v rámci procesu řízení rizik a obsahují:

- Přehled identifikovatelných aktiv, jejich klasifikace a určení odpovědnosti.
- Přehled nalezených rizik a slabých míst z hlediska bezpečnosti. Konkrétní rizika musí být doplněna o přehled hrozeb, včetně posouzení jejich závažnosti a o ohodnocení jejich vazby na konkrétní aktiva.
- Musí obsahovat konkrétní bezpečnostní opatření, včetně stanovení jejich priorit.
- Může obsahovat manažerský souhrn výsledků analýzy rizik včetně doporučení, jak s těmito závěry dále nakládat.

Analýza rizik tedy dále zpřesňuje odhad dopadů v závislosti na jejich četnosti a ukazuje nám místa, kde je nutno aplikovat ochranná opatření a jaké investice na jejich implementaci jsou adekvátní.

3.4 Aktiva

Aktiva organizace mají svoji hodnotu, která je v absolutní většině případů pro organizaci z hlediska jejího fungování kritická. V případě ztráty nebo závažného poškození některých aktiv tak může dojít i k ukončení činnosti organizace, a tím ke značným finančním ztrátám majitele nebo akcionářů, nemluvě o obchodních partnerech, zákaznících i zaměstnancích.

Aktivum může být komponenta nebo určitá část celého systému, které organizace přikládá určitou hodnotu a pro kterou je třeba mít nastavený způsob ochrany.[5] Mezi nejdůležitější aktiva řadíme:

[5] Je důležité si uvědomit, že aktivum nemusí být tvořeno hardwarem nebo softwarem.

- informace - data (klasicky zákaznický systém)
- hardware (PC, tiskárna, notebook)
- software (aplikace apod.)
- komunikační zařízení (sítě, telefony, modemy)
- dokumenty (smlouvy, zápisy apod.)
- personál (know how)
- image organizace

3.4.1 Identifikace aktiv

Aby mohlo být provedeno ohodnocení aktiv, musíme je nejprve identifikovat. V této etapě se doporučuje seskupit všechna aktiva, která k sobě logicky patří. Je nutné vždy identifikovat vlastníka každého daného aktiva (tzn. pověřenou osobu, plně odpovědnou za toto aktivum). S tímto vlastníkem posléze určujeme konkrétní hodnotu aktiva.

3.4.2 Ohodnocení aktiv

Identifikovaná aktiva je potřeba ohodnotit. Identifikace a ohodnocení aktiv organizace je základní krok v celkovém procesu analýzy rizik. Vlastní proces ohodnocení aktiv si každá organizace může nastavit sama podle svých potřeb, případně podle ČSN ISO/IEC TR 13335.

Při hodnocení aktiv se berou v úvahu následující hlediska: pořizovací náklady či jiná hodnota aktiva,

- důležitost aktiva pro existenci či chování subjektu,
- náklady na překlenutí případné škody na aktivu,
- rychlost odstranění případné škody na aktivu,
- jiná hlediska (mohou být specifická případ od případu)[6].

Dalším krokem je stanovení stupnice a hodnotící kritéria, které se použijí k ohodnocení určitého aktiva. Stupnice může být vyjádřena penězi nebo kvalitativními hodnotami. Je na uvážení jakou variantu zvolíme. Je možné také obě varianty kombinovat. Hlavním principem při ohodnocení aktiv jsou náklady vzniklé v důsledku porušení DŮVĚRNOSTI, INTEGRITY a DOSTUPNOSTI. Tedy tyto tři kritéria poskytují podklady

[6] Nejedná o zcela vyčerpávající seznam. Ve výrobní firmě to mohou být např. vyrobené součástky, v obchodě peníze apod.)

pro ohodnocení aktiv.
Některá aktiva mohou v průběhu hodnocení nabývat několik hodnot a to, podle kterého kritéria hodnotíme. Např. informační systém může být hodnocen z hlediska pořizovacích investic, z hlediska důvěrnosti a dostupnosti apod. Každá z definovaných hodnot se bude lišit. Finální přiřazená hodnota se může rovnat max. hodnotě ze všech uvedených, nebo může být průměrem nebo součtem. Zvolený model, musíte použít pro všechny aktiva, u nichž je využita kombinovaná hodnota. Stanovené hodnoty slouží jako základ pro analýzu rizik a výpočet nákladů na jejich ochranu.

3.4.3 Výpočet hodnoty aktiva

Pro výpočet ohodnocení aktiva je možno využít různé postupy. Nejjednodušším a také nejpoužívanějším je tzv. součtový algoritmus. Principem je součet: Dostupnost + Důvěrnost + Integrita /3. (x+y+z/3).Tento součtový algoritmus je nejrychlejší způsob získání hodnoty aktiva. Hodnoty aktiv určují dopad pro organizaci v případě zničení systému.

3.5 Hodnocení rizik

Podle pokynu Policejního prezidenta je každý útvar povinen zpracovat krizový plán pro účely zabezpečení činnosti útvaru pří mimořádných situacích. V tomto plánu musí být zahrnuty mimořádné situace, jako je např. povodeň, požár, dlouhodobá havárie dodávky vody, elektrické energie tepla apod.

Součástí tohoto plánu je hodnocení rizik pří mimořádných situacích, kde je uvedeno:

a) identifikace zdrojů rizika (nebezpečí),
b) určení možných scénářů událostí a jejich příčin, které mohou vyústit v závažnou havárii,
c) odhad dopadů možných scénářů závažných havárií na zdraví a životy lidí, hospodářská zvířata, životní prostředí a majetek,
d) odhad pravděpodobností scénářů závažných havárií,
e) stanovení míry rizika,
f) hodnocení přijatelnosti rizika vzniku závažných havárií.

3.5.1 Analýza rizik využívající matice aktiv, hrozeb a zranitelností

Pro analýzu rizik se používá několik základních přístupů. Jedním ze způsobů analýzy rizik je využití matice aktiv, hrozeb a zranitelností. Při této analýze rizik využijeme matici zranitelností a matice rizik. Do matice doplníme identifikované hrozby a jejich pravděpodobnosti. V dalším kroku posoudíme a doplníme zranitelnosti jednotlivých aktiv (skupin aktiv) jednotlivými hrozbami do matice zranitelností.

Posledním krokem analýzy je výpočet míry rizika podle vzorce R = T * A * V, kde

R - je míra rizika,

T - je pravděpodobnost vzniku hrozby,

A - je hodnota aktiva,

V - je zranitelnost daného aktiva.

Výpočty míry rizika a doplníme do matice rizik. Po analýze stanovíme hranice pro výši rizika podle stupnice: nízká (přijatelná), střední a vysoká rizika.

Analýza rizik se může provést pomocí metody vyhodnocující pravděpodobnost incidentu a jeho dopadu. Tímto postupem analýzy rizik se vyhodnotí pravděpodobnost incidentu a jeho dopad. Metoda využívá tři parametry (aktivum, hrozba a zranitelnost) nebo pouze dva parametry (pravděpodobnost a dopad incidentu).

Tato metoda je více popisná a musí pokrýt všechna identifikovaná aktiva. Zpracování je obdobné jako u předchozí metody. Doplníme identifikovaná aktiva a jejich hodnoty. K jednotlivým aktivům identifikujeme hrozby, zranitelnosti a existující opatření.

Odhadneme pravděpodobnost incidentu, který ohrozí dané aktivum. Pravděpodobnost a intenzita incidentu je snižována protiopatřeními.

Míra rizika je následně vypočtena podle vztahu R = PI x D.

PRAKTICKÁ ČÁST

4 BEZPEČNOST PERSONÁLNÍHO SYSTÉMU MV EKIS II.

Minimální bezpečnostní požadavky v oblasti počítačové bezpečnosti

- Jednoznačná identifikace a autentizace uživatele
- Nepřetržité zaznamenávání událostí, které mohou ovlivnit bezpečnost informačního systému, do auditních záznamů a zabezpečení těchto záznamů před neautorizovaným přístupem, zejména modifikací nebo zničením.
- Ochrana důvěrnosti dat během přenosu sítěmi.
- Zajištění odpovědnosti uživatele za jeho činnost v informačním systému.
- Řídit přístup k informacím podle povahy jeho pracovního zařazení (funkce a příslušnost k útvaru).
- Zpracování plánu na obnovení činnosti po havárii informačního systému a opětovné uvedení informačního systému do známého zabezpečeného stavu
- Organizování servisních činností v provozovaném informačním systému tak, aby nebyla ohrožena jeho bezpečnost.
- Stanovení termínů v bezpečnostní dokumentaci informačního systému a při vzniku krizové situace, kdy má být neprodleně prováděno vyhodnocování auditních záznamů.

4.1 Centrální část

Personální systém Ministerstva vnitra je provozován jako centrální systém. Veškerá data a aplikace jsou umístěna v centrální části systému na výpočetním středisku Ministerstva vnitra.

Výpočetní středisko je umístěno v takové budově ministerstva, která je chráněna před přírodními vlivy. V budově jsou instalovány protipožární ochrany a je zde také zajištěna stabilizovaná dodávka elektrické energie. Z pohledu fyzické bezpečnosti IS je tato budova zabezpečena dostatečně.

4.2 Pracovní stanice

Pracovní stanice jsou rozmístěny na pracovištích personálních oddělení Krajských ředitelství Policie ČR a útvarů policie s celorepublikovou působností a na všech pracovištích policie ČR kde je nutné plánovat služby. Celkový počet uživatelů systému EKIS II u policie je asi 8000. Všechna pracoviště jsou umístěna v budovách policie po celé republice. Vzhledem k velkému počtu pracovních stanic EKIS nelze každou pracovní stanici zabez-

pečit tak, aby byla funkční při některých mimořádných situacích. Musí se zajistit nouzový provoz informačního systému s nezbytnou funkcionalitou. Vzniklé mimořádné situace

4.3 Povodně 2002

4.3.1 Krajské ředitelství policie Plzeňského kraje

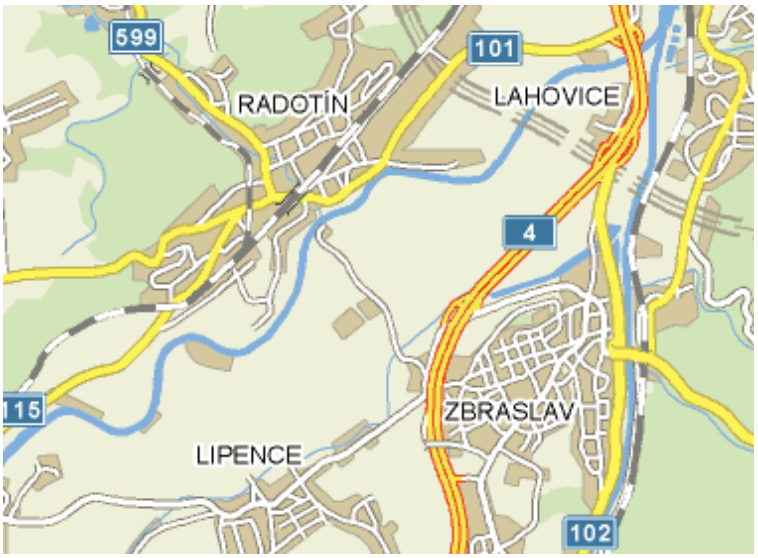
Obrázek 9 – Budova krajského ředitelství

Při povodni v roce 2002 došlo k zatopení objektu Krajského ředitelství policie Plzeňského kraje v Plzni Nádražní ulici. Objekt byl zatopen do úrovně 1 nadzemního podlaží. V důsledku toho došlo při zatopení k přerušení dodávky elektrické energie a výpadku výpočetní techniky a počítačových sítí. V tomto objektu je umístěno personální oddělení krajského ředitelství, pro jehož práci je důležitá funkční výpočetní technika. Následkem byl provoz personálního oddělení značně omezen. Personalisté z těchto důvodů nemohli vydávat potřebná personální opatření. Vzniklá situace byla řešena přepojením síťových prvků do míst, kde nebyl přerušen přívod elektrického proudu. Řešení této situace bylo improvizací a nebylo součástí žádného krizového plánu.

Obrázek 10 – Pohled na lokalitu krajského ředitelství

4.3.2 Krajské ředitelství policie Středočeského kraje

V roce 2002 došlo v důsledku vysoké vody v Berounce a ve Vltavě k znepřístupnění objektu Krajského ředitelství policie Středočeského kraje v areálu Na Baních Praha 5, Zbraslav. Areál se nachází na kopci, byl však nedostupný z důvodu zaplavení přístupových cest směrem od Prahy a přerušení městské hromadné dopravy v oblasti Praha – Smíchov. Pracoviště personalistů bylo přemístěno s nejnutnějšími materiály potřebnými k výkonu práce do jiného areálu Krajského ředitelství připojeného na síť kde personalisté po dobu nezbytně nutnou pracovali se systémem EKIS II. Mapy oblasti Praha Zbraslav jsou pro lepší ilustraci v příloze 5 – 6.



Obrázek 11 – Mapa oblast Praha Zbraslav

Obrázek 12 – Povodně 2002 v oblasti Praha Zbraslav

Vzhledem k tomu, že systém EKIS je centrální systém, přístupný z kteréhokoliv místa připojeného do sítě WAN Ministerstva vnitra bylo možné v obou případech zajistit náhradní spojení koncových stanic do této sítě.

5 ANALÝZA RIZIK

5.1 Identifikace aktiv EKIS

Jako první krok analýzy rizik jsem provedl identifikaci a ocenění aktiv. Pro účely této práce jsem vybral několik aktiv. Zpracoval jsem ukázkový přehled aktiv. Pro ukázku analýzy rizik nám postačí pouze několik aktiv. Pro ohodnocení aktiv je použita škála 1 až 5, přičemž nejdůležitější aktiva jsou označena „5“.

Ohodnocení aktiv a jejich identifikace je uvedena v seznamu Tabulka 5.
V tabulce jsou aktiva seskupena do skupin, které k sobě logicky patří. Ke každému aktivu byl přiřazen vlastník, respektive odbor ministerstva vnitra.

Typ aktiv	Identifikovaná aktiva	Hodnota aktiva	Majitel aktiv
Informace	Data na databázovém serveru R/3	5	Odbor personální
	Data na serveru Lotus Domino	5	Odbor personální
HW	Servery	4	Provoz informačních systémů
	PC	2	Provoz informačních systémů
SW	Operační systémy	3	Provoz informačních systémů
	Databázové systémy	3	Provoz informačních systémů
Služby	Připojení k serveru R/3	5	Provoz komunikačních služeb
	Připojení k serveru Lotus Domino	4	Provoz komunikačních služeb

Tabulka 5 - Identifikovaná aktiva

Pro analýzu rizik můžeme použít formulář uvedené v příloze 7 – 9.

5.2 Identifikace hrozeb a zranitelnost

Dalším krokem po identifikaci a ocenění aktiv je identifikace hrozeb a zranitelností. Pro aktiva identifikovaná v tabulce 5 jsem vytipoval několik hrozeb a zranitelností. V tabulce jsem uvedl pravděpodobnost jednotlivých hrozeb spolu s příklady zranitelností. Pro ohodnocení pravděpodobnosti hrozby byla opět použita škála 1 až 5, kdy nejpravděpodobnější hrozba je ohodnocena „5“. V tomto případě je nutné pamatovat na to, že jedna hrozba může využít více zranitelností a stejně tak jednu zranitelnost může využít více hrozeb.

Součástí tohoto plánu je hodnocení rizik pří mimořádných situací, kde je uvedeno:

a) identifikace zdrojů rizika (nebezpečí),

b) určení možných scénářů událostí a jejich příčin, které mohou vyústit v závažnou havárii,

c) odhad dopadů možných scénářů závažných havárií na zdraví a životy lidí, hospodářská zvířata, životní prostředí a majetek,

d) odhad pravděpodobností scénářů závažných havárií,

e) stanovení míry rizika,

f) hodnocení přijatelnosti rizika vzniku **závažných** havárií.

Identifikovaná hrozba	Pravděpodobnost hrozby	Příklad související se zranitelností
Selhání hardware	3	Náchylnost zařízení na vlhkost, prach a ušpinění
Selhání software	3	Nejasné nebo neúmyslné specifikace pro vývojáře
Zpronevěření aktiv	3	Nedostatek fyzické ochrany budov, dveří a oken
Zlomyslné kódy	5	Nedostatek aktualizací software na ochranu před zlomyslnými kódy
Neúmyslná modifikace	5	Nedostatečný výcvik bezpečnosti
Selhání komunikačních služeb	4	Nechráněná veřejná síťová připojení
Výpadek dodávky energií	3	Nedostatečná kapacita UPS, nefunkční náhradní zdroj
Požár	3	Funkčnost požárních hlásičů
Povodeň	2	Umístění v místech náchylných k povodním

Tabulka 6 - Identifikované hrozby a souvisejících se zranitelností

	Ppopis aktiva	Databáze serveru R/3	Databáze serveru Lotus Domino	Servery	PC	Operační systémy	Databázové systémy	Připojení k serveru R/3	Připojení k serveru Lotus
	Hodnota aktiva	**5**	**5**	**4**	**2**	**3**	**3**	**5**	**4**
Popis hrozby	**Pravděpodobnost hrozby**								
Selhání hardware	**3**			2	2				
Selhání software	**3**					2	2		
Zpronevěření aktiv	**3**			2	2				
Povodeň	**2**			1	1			4	4
Zlomyslné kódy	**5**					2	2		
Neúmyslná modifikace	**5**	2	2						
Selhání komunikačních služeb	**4**							5	4
Výpadek dodávky energií	**3**							3	3

Tabulka 7 - Tabulka matice zranitelností

Pro ohodnocení rizika se dají využít dotazníky uvedené v přílohách 7-9. Dotazníky se týkají vybraných hrozeb:

- **Požár**

  Míra zranitelnosti budovy a místnosti vůči požáru závisí na rozsahu, na který se požár po vypuknutí může rozšířit.
- **Poškození vodou**

  Míra zranitelnosti budovy a místnosti vůči poškození vodou závisí na rozsahu, v jakém může voda zatopit místnost.
- **Přírodní katastrofa**

  Hrozba přírodní katastrofy pokrývá poškození lokality nebo jejího prostředí incidentem způsobeném přírodními poměry (záplava) nebo lidmi (dopravní nehoda).

Všechny tyto hrozby mohou poškodit libovolná fyzická aktiva systému (včetně dokumentace a magnetických médií). Stupeň poškození závisí na rozsahu poškození zařízení a na tom do jaké míry to naruší funkčnost organizace.

6 NÁVRHY NA BEZPEČNOSTNÍ OPATŘENÍ

Z výše uvedeného vyplývá, že EKIS II. je pro práci personálních pracovišť důležitý a bez tohoto systému není možné vydávat žádná personální opatření. Jakékoliv náhradní řešení jako např. psaní personálních opatření v textovém editoru nebo plánování služeb v listinné podobě může mít za následek nekonzistenci v datech personálního systému. Tato nekonzistence může mít za následek i značné finanční dopady a to vzhledem k počtu zpracovávaných dat jak pro policisty, tak pro ministerstvo vnitra. Neméně důležitý je tento systém pro pracovníky, kteří plánují služby policistů. Celkový počet těchto pracovníkům se pohybuje okolo 8000 pracovníků.

Na základě výše uvedených údajů je zapotřebí zajistit bezporuchový třeba i částečně omezený provoz informačního systému informačního systému.

Na základě pokynu oddělení krizového řízení PP ČR se v současné době nově zpracovávají krizové plány pro jednotlivé objekty Policie ČR. V těchto plánech není zahrnuto řešení zabezpečení pracovišť, kde je provozován systém EKIS. Ministerstvo vnitra, provozovatel systému EKIS řešilo pouze bezpečnost centrální části systému.

Je důležité zpracovat krizové scénáře pro provoz výše uvedených pracovišť při mimořádných situacích. Tyto scénáře musí obsahovat:

a) Opatření následující bezprostředně po vzniku krizové situace zaměřená na minimalizaci škod, způsob zajištění nouzového provozu informačního systému s vyjmenováním minimálních funkcí, které musí být zachovány,

b) Opatření vedoucí k uvedení systému do známého bezpečného stavu.

Na všechna pracoviště nelze možné řešit jednotnými postupy, ale řešení musí odpovídat lokalitě a místním poměrům. V bezpečnostní dokumentaci informačního systému musí být uvedeny postupy s osobní odpovědností jednotlivých pracovníků. Jako vzor uvádím tabulku „Rozpis činnosti pracovníků útvaru při mimořádné situaci“.

Bezpečnostní dokumentaci musí zpracovat jednotlivá pracoviště ve spolupráci s IT specialisty Ministerstva vnitra, kteří spravují systém EKIS a se specialisty na počítačové sítě.

Rozpis činnosti pracovníků útvaru při mimořádné situaci

Odpovědná osoba	Činnost
Ředitel krajského ředitelství / ředitel útvaru	Rozhodne podle závažnosti havárie o náhradním provozu, nebo o jeho případném omezení. Uloží úkoly dalším podřízeným pracovníkům
Vedoucí personálního oddělení	Rozdělí jednotlivé činnosti konkrétním pracovníkům Zajistí informovanost klientů o vzniklé situaci a o náhradním provozu
Personalista	Zajistí si nezbytně nutné dokumenty pro svoji práci Bude vykonávat činnosti určené vedoucím personálního oddělení
Správce počítačových sítí	Podle závažnosti havárie zajistí náhradní připojení nezbytně nutného počtu počítačů do rezortní počítačové sítě
Správce objektu	Zajistí náhradní prostory pro náhradní provoz personálního pracoviště po nezbytně nutnou dobu
Klienti policista/občanský zaměstnanec	Zahájí neprodleně práce k odstranění havárie byť jenom provizorním způsobem (Mobilní zdroj elektrické energie, náhradní vytápění apod.) V případě závažnější havárie případně zajistí v objektu náhradní prostory. Pokud to není v jeho silách, nahlásí to řediteli útvaru, který rozhodne o dalším postupu
Klienti policista/občanský zaměstnanec	V době mimořádné situace omezí vyřizovaní náležitostí na personálním oddělení na nezbytně nutné úkony

Tabulka 8 - Mimořádná situace - Rozpis činností - vzor

7 ZÁVĚR

Cílem této diplomové práce bylo zorientování se v problematice bezpečnosti informačních systémů, v práci policie při mimořádných situacích a poté navrhnout bezpečnostní opatření pro provoz informačního systému EKIS při těchto situacích.

Vzhledem ke způsobu práce policie a pro dodržení výše uvedených zákonných norem je nutné zabezpečit provoz informačního systému i při mimořádných situacích a to byť jenom v omezeném a nezbytně nutném rozsahu. K tomuto účelu je nutné navrhnout potřebná opatření zaměřená na zabezpečení provozu při mimořádných situacích. Součástí těchto opatření musí být určení jednoznačné odpovědnosti za jednotlivé části informačního systému. Na základě této odpovědnosti je zapotřebí zpracovat scénáře pro řešení mimořádné situace. Tato scénáře musí být uvedeny v bezpečnostní dokumentaci informačního systému a ve vnitřním havarijním plánu areálu a musí obsahovat:

- řešení nouzového provozu v omezeném rozsahu umožňující zabezpečit nutný chod policejních útvarů,
- činnosti následující bezprostředně po vzniku krizové situace zaměřená na minimalizaci škod,
- způsob zajištění nouzového provozu informačního systému s vyjmenováním minimálních funkcí, které musí být zachovány,
- činnost po vzniku mimořádné situace zaměřená na likvidaci následků mimořádné situace včetně vymezení osobní odpovědnosti za jednotlivé úkoly,
- způsob zálohování informačního systému,
- způsob zajišťování servisní činnosti,
- způsob obnovy funkčnosti a uvedení informačního systému do známého bezpečného stavu a to v co nejkratší době.

Zpracování těchto pravidel se týká, jak provozovatele tzn. Ministerstva vnitra, tak jednotlivých útvarů Policie ČR. V současné době nejsou tato pravidla v rezortu ministerstva vnitra zpracována.

SEZNAM POUŽITÉ LITERATURY

[1] DOBDA, L. Ochrana dat v informačních systémech. Praha: Grada, 1998. ISBN 80-7169-479-7

[2] POŽÁR, L. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005. ISBN 80-86898-38-5

[3] VALÁŠEK J., KOVAŘÍK F. A KOLEKTIV, Krizové řízení při nevojenských krizových situacích, MV - generální ředitelství HZS ČR, 2008. ISBN 987-80-86640-93-8

[4] PUŽMANOVÁ R., Moderní komunikační sítě od A do Z, Brno, Computer press, a.s., 2006, ISBN 80-251-1278-0

[5] SMEJKAL V., RAIS K. Řízení rizik ve firmách a jiných organizacích Praha: Grada, 2009. ISBN 978-80-247-3051-6

[6] Zákon č. 273/2008 Sb. ze dne 17. července 2008 o Policii České republiky

[7] Zákon č. 361/2003 Sb. ze dne 23. září 2003 o služebním poměru příslušníků bezpečnostních sborů

[8] Zákon č. 101/2000 Sb. ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů.

[9] Bezpečnost IS - co to znamená? (1. díl)Bezpečnost (10.10.2004) http://www.isvs.cz/bezpecnost/bezpecnost-is-co-to-znamena-1-dil-.html

[10] Bezpečnostní politika (2. díl) (20. 10. 2004) http://www.isvs.cz/bezpecnost/bezpecnostni-politika-2-dil-.html

[11] Bezpečnost informačních systémů - rizika (3. díl) (02. 11. 2004) http://www.isvs.cz/bezpecnost/bezpecnost-informacnich-systemu-rizika-3-dil-.html

[12] http://www.businessinfo.cz/cz/clanek/podnikatelske-prostredi/co-je-to-riziko-a-analyza-rizik/1001234/42740/

[13] MINICHBAUER J., Ochrana dat v ekonomickém informačním systému ministerstva vnitra - Bakalářská práce Policejní akademie v Praze, Praha - 2007,

[14] MINICHBAUER J., Ochrana dat v ekonomickém informačním systému ministerstva vnitra - Učební texty pro předmět Manažerská informatika Policejní akademie v Praze, Praha - 2007

[15] Nařízení Ministerstva vnitra č. 20/2007 ze dne 14. února 2007 o personální evidenci a o zpracovávání osobních údajů, které s ní souvisejí.

[16] MATYÁŠ V. Příručka manažera VIII. – Autentizace uživatelů a autorizace elektronických transakcí, TATE Internationál, s.r.o., 2007

[17] BS – 7799 British Standard Institute Information Security Management a IEC 17799 pro řízení informační bezpečnosti a certifikace systémů ISMS - Překlad a interpretace pro české prostředí, Risk Analysis Consultants, s.r.o., 2002

SEZNAM POUŽITÝCH POJMŮ

Resort Ministerstva vnitra - souhrn útvarů Ministerstva vnitra, útvarů Policie ČR, organizačních složek státu, státních příspěvkových organizací, ústavů, účelových zařízení, azylových zařízení

Útvar resortu MV - organizační jednotka, v jejímž čele stojí vedoucí zaměstnanec s personální pravomocí.

Organizační jednotka - podmnožina organizačních subjektů resortu zřízená k zajištění úkolů resortu, řízená vedoucím zaměstnancem. Elementární dále nedělitelná nebo agregovaná (složená z několika elementárních nebo agregovaných jednotek).

Občanský zaměstnanec - je zaměstnanec v pracovním poměru k Ministerstvu vnitra, k Policii ČR, k příspěvkovým organizacím a k organizačním složkám státu zřizovaným Ministerstvem vnitra, občanský zaměstnanec v pracovním poměru k Ministerstvu vnitra (generální ředitelství HZS) a k Hasičskému záchrannému sboru ČR.

Příslušník P ČR - je příslušník Policie ČR ve služebním poměru.

Příslušník HZS ČR - příslušník Hasičského záchranného sboru ČR ve služebním poměru.

Příslušník - příslušník P ČR a příslušník HZS ČR.

Zaměstnanec - je občanský zaměstnanec a příslušník.

Vedoucí zaměstnanec - zaměstnanec pověřený vedením jiných zaměstnanců

Nadřízený vedoucí zaměstnanec - řídí činnost více útvarů resortu MV

Vedoucí zaměstnanec - přímý nadřízený - je oprávněn organizovat, řídit a kontrolovat práci podřízených zaměstnanců,

Vedoucí zaměstnanec s personální pravomocí - je oprávněn činit právní úkony v pracovně právních vztazích, je oprávněn rozhodovat ve věcech služebního poměru podřízených zaměstnanců, (ministr vnitra, vedoucí zaměstnanec ministerstva - náměstek, generální ředitel Hasičského záchranného sboru ČR, ředitel útvaru, policejní prezident P ČR, služební funkcionář – PP ČR, útvarů P ČR s celorepublikovou působností ředitel útvaru policie, služební funkcionáři krajských ředitelství P ČR, ředitel policejní školy, rektor policejní akademie, ředitel organizační složky státu a státní příspěvkové organizace).

Oprávněný zaměstnanec - zaměstnanec určený k využívání IS s přidělenými přístupovými právy odpovídajícími rozsahu jeho činnosti definované organizačním řádem, resortními předpisy, provozním řádem EKIS a jeho popisem práce.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

EKIS Ekonomický informační systém Ministerstva vnitra

EKIS I Část ekonomického EKIS obsahující moduly pro vedení finančního účetnictví a materiálových evidencí včetně vnitropodnikového účetnictví.

EKIS II Část ekonomického EKIS obsahující moduly obsahující personální a mzdovou agendu včetně systemizace a vzdělávání.

PP ČR Policejní prezidium České republiky

P ČR Policie ČR

HZS ČR Hasičský záchranný sbor ČR

MV Ministerstvo vnitra

GŘ HZS Generální ředitelství hasičského záchranného sboru

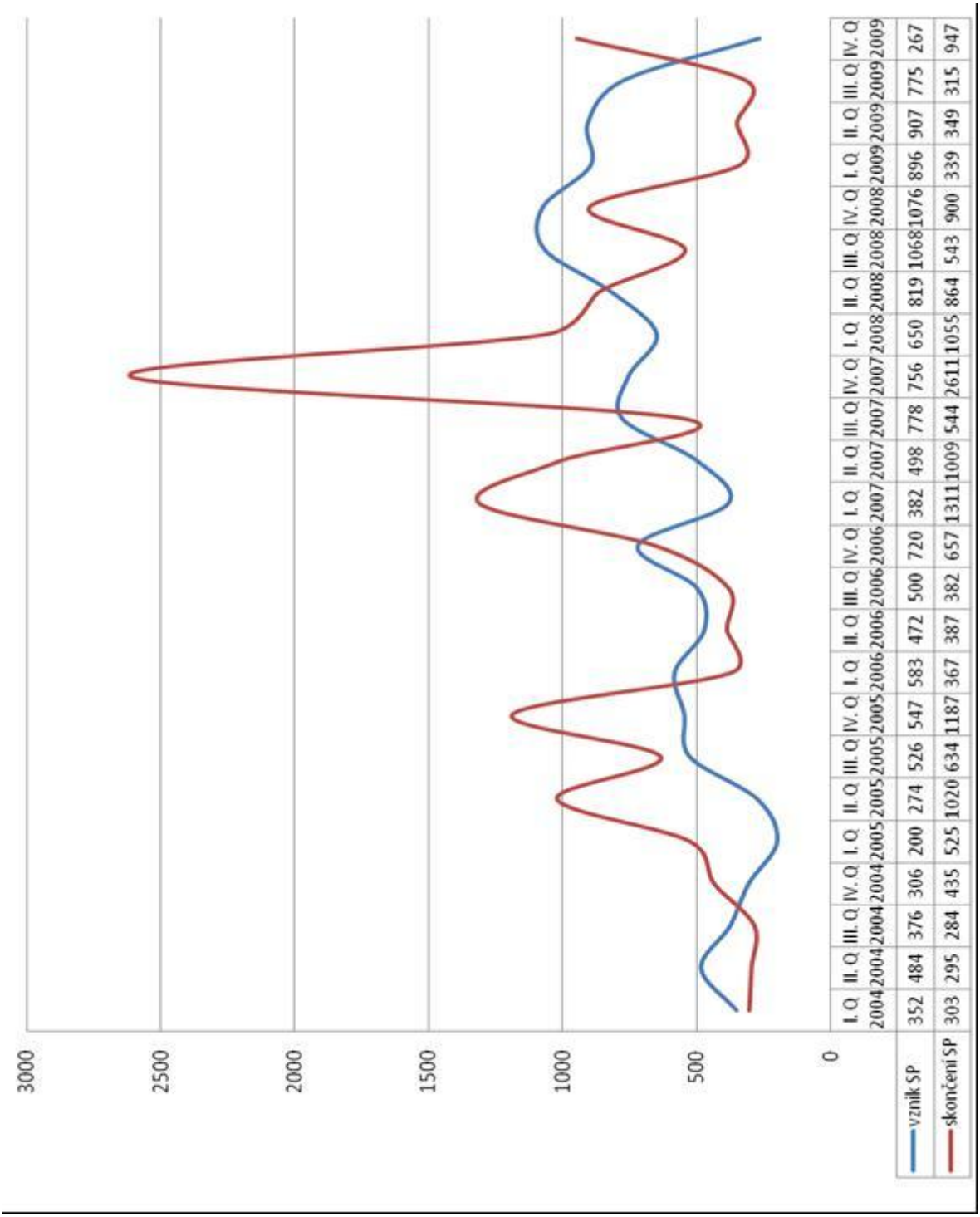
NMV Nařízení Ministerstva vnitra

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

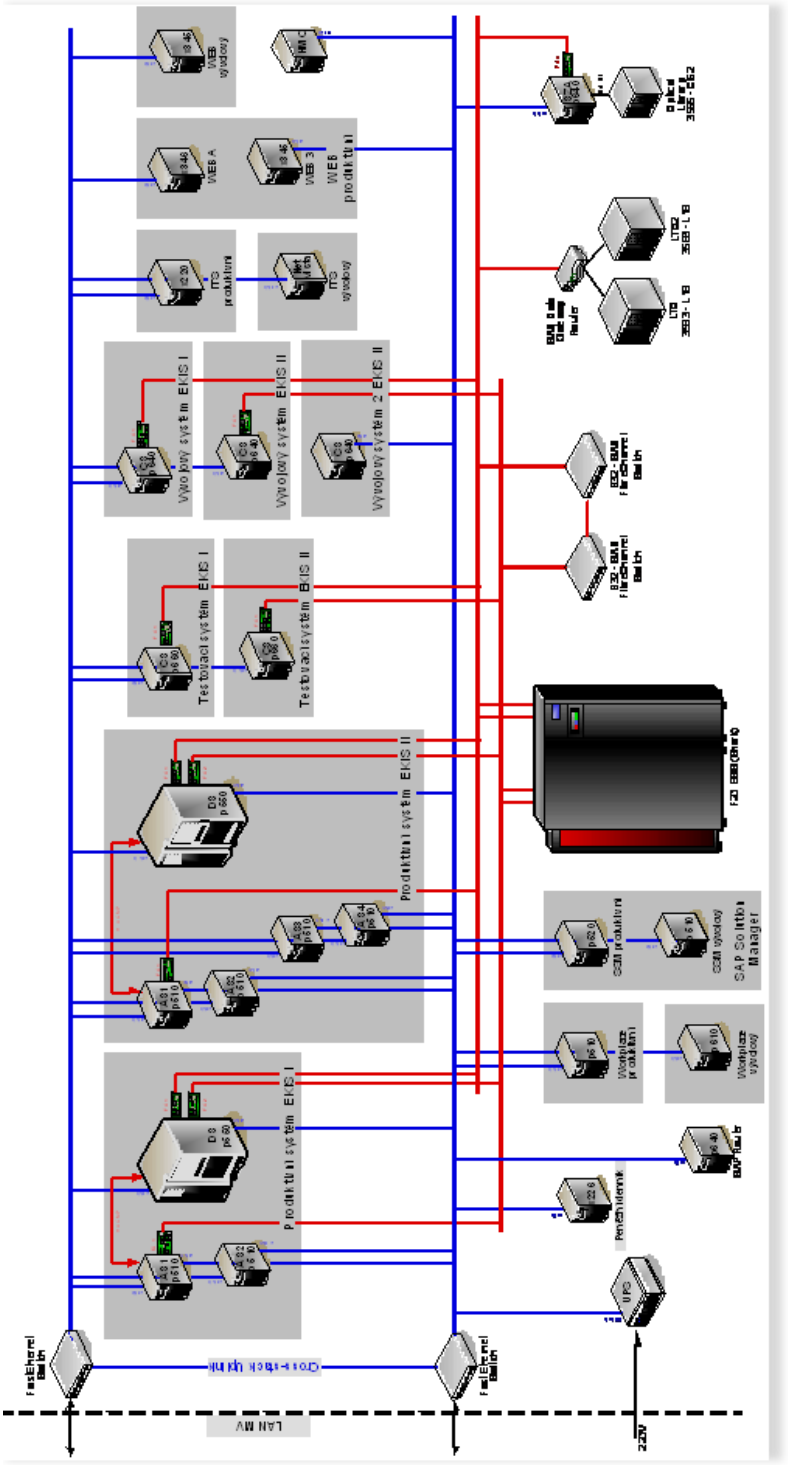
SEZNAM PŘÍLOH

Příloha 1 - Skončení a vznik služebního poměru



	I. Q 2004	II. Q 2004	III. Q 2004	IV. Q 2004	I. Q 2005	II. Q 2005	III. Q 2005	IV. Q 2005	I. Q 2006	II. Q 2006	III. Q 2006	IV. Q 2006	I. Q 2007	II. Q 2007	III. Q 2007	IV. Q 2007	I. Q 2008	II. Q 2008	III. Q 2008	IV. Q 2008	I. Q 2009	II. Q 2009	III. Q 2009	IV. Q 2009
vznik SP	352	484	376	306	200	274	526	547	583	472	500	720	382	498	778	756	650	819	1068	1076	896	907	775	267
skončení SP	303	295	284	435	525	1020	634	1187	367	387	382	657	1311	1009	544	2611	1055	864	543	900	339	349	315	947

Příloha 2 - Architektura centrální části



Příloha 3 – Aktiva

	AKTIVA
1	**Policie ČR**
1.1	Policie ČR - výkonné složky
1.2	Krajské ředitelství policie ČR
2	**Ostatní záchranné, zdravotní a hygienické služby**
2.1	Regionální státní ústav pro jadernou bezpečnost
2.2	Pobočka českého hydrometeorologického ústavu
2.3	Povodí
2.4	Krajská hygienická stanice
2.5	Krajská veterinární správa
2.6	Humanitární organizace
2.7	Pohřební služby
3	**Ochrana, varování a informování obyvatel**
3.1	Úkryty pro obyvatelstvo
3.2	Sklady materiálu civilní ochrany
3.3	Prostředky individuální ochrany pro vybrané skupiny
3.4	Systémy varování obyvatelstva (sirény)
3.5	Rozhlas, televize, deníky
4	**Komunikační a podpůrné systémy**
4.1	Internet/intranet
4.2	Mobilní, krizové telefony
4.3	Vysílačky
4.4	Systémy elektronické pošty (mail)
4.5	Informační systémy pro podporu rozhodování
4.6	Telefonní ústředny - JTS
4.7	Ústředny mobilních operátorů
5	**Ubytovací zařízení**
5.1	Obytné domy
5.2	Hotely, motely
5.3	Ubytovny, hostely, studentské koleje
5.4	Kempy a rekreační zařízení
5.5	Nouzové ubytování
5.6	Rezerva 1
6	**Stravovací zařízení**
6.1	Restaurace
6.2	Jídelny, vývařovny
6.3	Závodní a školní jídelny
6.4	Mobilní kuchyně
7	**Zásobování pitnou vodou**
7.1	Zdroje pitné vody
7.2	Vodárny, vodojemy
7.3	Vodovody
7.4	Cisterny na pitnou vodu

8	**Zásobování elektřinou, teplem**
8.1	Elektrárny tepelné, vodní
8.2	Elektrárny jaderné
8.3	Elektrické rozvodny, trafostanice
8.4	Elektrorozvodná síť
8.5	Mobilní elektrocentrály
8.6	Teplárny
8.7	Teplovody
9	**Dopravní prostředky - přeprava osob**
9.1	Autobusy
9.2	Osobní auta
9.3	Vlaky pro osobní přepravu
10	**Odpadové hospodářství**
10.1	Čistírny odpadních vod
10.2	Kanalizace
11	**Dopravní trasy**
11.1	Dálnice
11.2	Silnice
11.3	Železnice
1.14	Vodní toky

Příloha 4 - Seznam hrozeb

	Hrozby informačního systému
.	Živelní pohromy
1.1	Požár (přírodního i lidského původu)
1.2	Záplavy a povodně (deště, tání sněhu, protržení hráze)
1.3	Vichřice, větrné smršťě, tornáda
1.4	Blesky (a další elektrické jevy v atmosféře)
1.5	Krupobití, přívalové deště
1.6	Sněhové vánice a kalamity
1.7	Extrémní vedra a sucha
1.8	Silné mrazy
1.9	Námrazy, náledí, ledovky, mrznoucí déšť
1.10	Teplotní inverze (špatné rozptylové podmínky)
1.11	Sesuvy půdy a skalních bloků
1.12	Sněhové a kamenné laviny
1.13	Epidemie, pandemie
1.14	Zanášení koryt vodních toků
1.15	Půdní eroze
1.16	Propady zemského povrchu (přírodní dutiny, důlní činnost, …)
1.17	Zemětřesení
1.18	Únik důlních plynů ze zemského nitra
1.19	Zvýšená přírodní radioaktivita (naleziště uranu, únik radonu)
1.20	Geomagnetické bouře
1.21	Kosmické záření, UV záření (ozónová díra)
1.2	Pád kosmického tělesa
2.	Průmyslové a dopravní havárie
2.1	Dopravní havárie
2.2	Dopravní havárie s následným výbuchem
2.3	Dopravní havárie s následným požárem
2.4	Dopravní havárie s následným únikem ropných produktů
2.5	Dopravní havárie s následným únikem toxických látek
2.6	Dopravní havárie s následným únikem radioaktivních látek
2.7	Provozní havárie
2.8	Provozní havárie s následným výbuchem
2.9	Provozní havárie s následným požárem
2.10	Provozní havárie s následným únikem ropných produktů
2.11	Provozní havárie s následným únikem toxických látek
2.12	Provozní havárie s následným únikem radioaktivních látek
3.	Technická selhání
3.1	Destrukce staveb
3.2	Technické poruchy/selhání

3.3	Mechanická poškození
3.4	Nefunkční spojení
4.	Organizační nedostatky
4.1	Narušení zásobování
4.2	Narušení výrobních procesů
4.3	Nedostatečné kapacity/zdroje
4.4	Nedostatek pracovní síly
4.5	Nedostatek kvalifikované pracovní síly
4.6	Nedostupnost služeb
4.7	Nedostatečné finanční zdroje
4.8	Chybná interpersonální komunikace
5.	Úmyslná škodlivá lidská činnost
5.1	Teroristický útok
5.2	Sabotáž
5.3	Velké veřejné akce, demonstrace
5.4	Stávka
5.5	Hromadné násilí
5.6	Rabování
5.7	Vandalismus
5.8	Násilná kriminální činnost
5.9	Krádež
6.	Negativní dopady lidské činnosti
6.1	Působení chemických prostředků v zemědělství
6.2	Průsaky ze skládek komunálních odpadů
6.3	Průsaky ze skládek toxických odpadů
6.4	Znečištění ovzduší prachem
6.5	Nadměrný hluk a vibrace
6.6	Nelegální skládky nebezpečného odpadu
7.	Vyšší moc
7.1	Změna politického klimatu
7.2	Změna legislativy
7.3	Náhlá ztráta/úbytek osob
7.4	Migrační vlny
7.5	Záchranné / humanitární akce

Příloha 5- Mapa oblasti Praha Zbraslav

Příloha 6 - Fotografická mapa oblasti Praha Zbraslav

Příloha 7- Hrozba požáru

Hrozba požáru pokrývá incident poškození libovolných fyzických aktiv systému (včetně dokumentace a magnetických médií) požárem. Míra zranitelnosti budovy a místnosti vůči požáru závisí na rozsahu, na který se požár po vypuknutí může rozšířit, a na míře s jakou naruší fungování organizace.

1. **Kolik požáru libovolného typu se vyskytlo za poslední 3 roky?**
   - a Žádný 0
   - b Jeden nebo dva 10
   - c V průměru jeden ročně 20
   - d V průměru více než jeden ročně 50
   - e Neznámo 0
2. **Existují v okolí potenciální rizika požáru (např. vařiče)?**
   - a Ano 5
   - b Ne 0
3. **Je v blízkém okolí kritického zařízení IT dovoleno kouřit?**
   - a Ano 20
   - b Ne 0
4. **Existují zde nějaké prototypové nebo nestandardní prostředky, které by zvyšovaly pravděpodobnost požáru (např. vývojové práce nebo zastaralé elektrické rozvody)?**
   - a Ano 10
   - b Ne 0
5. **Nacházejí se v okolí vysoce rizikové budovy či uvnitř společné budovy organizace, které by mohly zvyšovat riziko šíření požáru (např. benzínové stanice, tiskárna)?**
   - a Ano 10
   - b Ne 0

6. Nacházejí se v okolí palivové nádrže, které nevyhovují požárním předpisům?

a Ano 10

b Ne 0

7. Je k dispozici dostatek přípojek napájení odpovídající provozním požadavkům? (Berte v úvahu přetížení zásuvek.)

a Ano 0

b Ne 5

8. Jaký je trend v počtu požárů?

a Rostoucí 10

b Zůstává nezměněn 0

c Klesající -10

9. Jaká je konstrukce budovy?

a Betonová / cihlová 0

b Jiná 10

10. Má budova hořlavý vnější obal (např. dřevěný plášť, popínavé rostliny atd.)?

a Ano 10

b Ne 0

11. Jsou místnosti špatně vybaveny (např. nedoléhající dveře nebo okna)?

a Ano 4

b Ne 0

12. Jsou v okolí kritického zařízení uloženy, zpracovány nebo přepravovány hořlavé materiály např. rozpouštědla, papírový odpad, balící materiály? (Neberte v úvahu malá množství pro běžné užívání.)

a Ano 10

b Ne 0

13. Jak jednoduše by se mohl požár v budově šířit? (Berte v úvahu volné prostory, vzduchotechnické potrubí ve zdech a stropech)

a Velmi rychle 25

b Rychle 10

c Pomalu 0

14. Existují z poslední požární prohlídky nevyřešená doporučení?

a	Ano - hlavní doporučení	25
b	Ano - vedlejší doporučení	10
c	Ne	0

15. Jaká je předpokládaná doba reakce hasičského sboru?

a	Méně než 5 minut	0
b	5 - 9 minut	5
c	10 - 14 minut	10
d	15 - 20 minut	15
e	Více než 20 minut	20

16. V jakém rozsahu může požár v této oblasti ovlivnit fungování organizace?

a	Žádné podstatné následky	0
b	Přerušení normální práce	10
c	Zdržení důležité práce	15
d	Přerušení kritické práce	20

Příloha 8 - Hrozba poškození vodou

Hrozba poškození vodou pokrývá incident, při němž by mohla fyzických aktiv systému (včetně dokumentace a magnetických médií) poškozena vodou.
Míra zranitelnosti budovy a místnosti vůči poškození vodou závisí na rozsahu, v jakém může voda zatopit místnost, na rozsahu v jakém může poškodit zařízení a na tom do jaké míry naruší funkčnost organizace.

1. **Kolik případů poškození vodou se vyskytlo za poslední tři roky?**

a	Žádný	0
b	Jeden nebo dva	10
c	V průměru jeden ročně	20
d	V průměru vícekrát za rok	50
e	Neznámý počet	0

2. **Jaký je trend v počtu případů poškození vodou?**

a	Rostoucí	10
b	Zůstává nezměněn	0
c	Klesající	-10

3. **Nachází se v místnosti s klíčovými prostředky IT nebo nad ní potrubí s vodou? (Berte v úvahu centrální vytápění, klimatizaci, vodovodní potrubí, odpad.)**

a	Ano	25
b	Ne	0

4. **Nacházejí se v budově nádrže vody, ze kterých by mohla potenciálně uniknout voda, a poškodit kritické zařízení IT?**

a	Ano	10
b	Ne	0

5. **Mohla by se v budově nahromadit voda a ohrozit kritické zařízení? (Berte v úvahu vliv silného deště na plochou střechu, selhání hydrantu atd.)**

a	Ano	10
b	Ne	0

6. **Mohlo by rozvodnění blízké řeky nebo nádrže poškodit kritické zařízení?**

a	Ano	10
b	Ne	0

7. Jsou místnosti, které obsahují kritická zařízení, špatně vybaveny (např. nedoléhající okna, měděná potrubí atd.)?

a	Ano	10
b	Ne	0

8. Jsou některé místnosti, kde je umístěno kritické vybavení, pod vodní hladinou?

a	Ano	10
b	Ne	0

9. Jsou některé místnosti, kde je umístěno kritické vybavení, v podzemí?

a	Ano	10
b	Ne	0

10. Jaký vliv na chod organizace by mělo poškození vodou?

a	Přerušení kritické práce	20
b	Zdržení důležité práce	15
c	Přerušení normálních činností	10
d	Žádné podstatné následky	0

Příloha 9 - Hrozba přírodní katastrofy

Hrozba přírodní katastrofy pokrývá poškození lokality nebo jejího prostředí incidentem způsobeném přírodní poměry (záplava) nebo lidmi (dopravní nehoda). Míra zranitelnosti prostředí nebo lokality závisí na rozsahu, s jakým katastrofa ovlivní chod organizace.

Mohla by být budova zasažena následujícími vlivy?

a	Silný vítr	10
b	Sesuv pudy/pokles terénu	10
c	Elektrické bouře	10
d	Padání těžkého sněhu	10
e	Extrémní teploty	10
f	Otřesy nebo vibrace	10
g	Ochromení dopravou	10
h	Monzun / silný déšť	10
i	Žádný z výše uvedených	0

11. Kolikrát za poslední tři roky byla lokalita postižena přírodní katastrofou?

a	Nikdy	0
b	Jednou nebo dvakrát	10
c	V průměru jednou ročně	20
d	V průměru více než jednou ročně	30
e	Neznámo kolikrát	0

12. Jaký je trend v počtu přírodních katastrof?

a	Rostoucí	10
b	Zůstává nezměněn	0
c	Klesající	-10

13. Jaký vliv by měla přírodní katastrofa na fungování organizace?

a	Přerušení kritické práce	20
b	Zdržení důležité práce	15
c	Přerušení normální práce	10
d	Žádné podstatné následky	0