Bezpečnostný prieskum, nástroj pre poznanie a analýzu bezpečnostnej situácie

Security survey, the tool for understanding and analyzing of the security situation

Daniel Bednárik

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Daniel BEDNÁRIK**
Osobní číslo:	**A09447**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnostní průzkum,nástroj pro poznání a analýzu bezpečnostní situace**

Zásady pro vypracování:

Cíl: Poskytnout bezpečnostním manažerům návod postupu při plánování a realizaci bezpečnostního průzkumu v terénu.

1. **Organizační aspekty bezpečnostního průzkumu (cíl,fáze,syntéza).**
2. **Psychologické a psychoanalytické aspekty postupu.**
3. **Metody bezpezpečnostního průzkumu.**
4. **Model,simulace bezpečnostního průzkumu u fiktivní organizace ke zpracování bezpečnostního projektu informační bezpečnosti.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. Broder, James F. Risk Analysis and Security Survey. Burlington, MA 01803, USA : Butterworth-Heinemann is an imprint of Elsevier, 2006. ISBN 13: 978-0-7506-7922-0.
2. LAUCKÝ, V. Řízení technologických procesů v PKB. Zlín : Academia centrum UTB, 2004.
3. LAUCKÝ, V. Technologie komerční bezpečnosti II. Zlín : Academia centrum UTB, 2004.
4. ISO/IEC 27001: 2005 Informačné technológie, zabezpečovacie techniky, systémy manažérstva informačnej bezpečnosti: požiadavky. Bratislava : Slovenský ústav technickej normalizácie, 2006.
5. ISO/IEC 27002: 2005 Informačné technológie, zabezpečovacie techniky, pravidlá dobrej praxe manažérstva informačnej bezpečnosti. Bratislava : Slovenský ústav technickej normalizácie, 2006.
6. TNI ISO/IEC TR 13335-3. Bratislava : Slovenský ústav technickej normalizácie, 2002.
7. Černý, Vojtěch. Prodejní techniky. Brno : Computer Press, 2003. ISBN 80-251-0032-4.

Vedoucí diplomové práce: **JUDr. Vladimír Laucký**
Ústav bezpečnostního inženýrství

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

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cieľom diplomovej práce je poskytnúť nástroj bezpečnostným konzultantom pre realizáciu bezpečnostného prieskumu. Zahrnutá je v nej problematika organizačných aspektov bezpečnostného prieskumu, ktorá zahŕňa prípravnú fázu na bezpečnostný prieskum, projekt manažment, prípravu dokumentácie, výber metód bezpečnostného prieskumu. Je venovaný priestor aj problematike psychologických aspektov prieskumu, ako je komunikácia a metodika zvládania konfliktov. Popisované metódy bezpečnostného prieskumu sú volené vzhľadom na praktickú využiteľnosť pre menšie organizácie, ktoré prieskum realizujú vzhľadom na ich možnosti z pohľadu know how, dostupnosti ľudských zdrojov, ekonomických možností a časového rámca pre realizáciu bezpečnostného prieskumu. V praktickej časti je simulovaný bezpečnostný prieskum s cieľom získania informácii pre zavedenie systému riadenia informačnej bezpečnosti. Informácie sú čerpané priamo z praxe, sú vysvetlené organizačné aspekty prieskumu. Je riešená problematika nastavenia metrík hodnotenia výsledkov bezpečnostného prieskumu. Pre syntézu sú vybrané dve bezpečnostné oblasti ako príklady.

Kľúčové slová: bezpečnostný prieskum, metódy bezpečnostný prieskum, analýza bezpečnosti, syntéza bezpečnosti, analýza rizík, prieskum bezpečnosti, bezpečnostné opatrenia.

ABSTRACT

The aim of this work is to provide a tool for implementing security consultant security survey. Included therein is the issue of organizational aspects of the security survey, which includes a preparatory phase to a security survey, project management protects, preparation of documentation, selection methods for research on security. Described are psychological aspects of the survey, such as communication and conflict management methodology. Described method for research on security are chosen with regard to the practicality of the smaller organizations that carry out exploration in respect of their options in terms of know-how, availability of human resources, economic potential and timeframe for implementation of safety survey. The practical part is simulated by a security survey to gather information for the implementation of information security management system. The information is drawn directly from practice, explained the organizational aspects of the survey. The thesis is dealing with setting metrics evaluating the results of safety research. As examples are selected two security areas for the synthesis.

Keywords: security survey, security surveys methods, security research, safety analysis, safety synthesis, risk analysis, safety precautions.

Ďakujem, vedúcemu práce pánovi Lauckému za odborné vedenie počas tvorby diplomovej práce.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Skúsení bezpečnostní špecialisti hodnotia výsledky takmer intuitívne často správne a s malými chybami. Pri menších skúsenostiach je možné túto neskúsenosť aspoň z časti nahradiť dobre štruktúrovaným, formalizovaným a organizovaným prístupom k analýze a následnej syntéze získaných výsledkov. Cieľom tejto práce je poskytnúť bezpečnostným špecialistom návod na organizované, štruktúrované, formalizované vykonanie bezpečnostného prieskumu. Bezpečnostný prieskum patrí do činnosti analytických útvarov priemyslu komerčnej bezpečnosti.

I. TEORETICKÁ ČASŤ

1 ORGANIZAČNÉ ASPEKTY BEZPEČNOSTNÉHO PRIESKUMU

1.1 Cieľ bezpečnostného prieskumu

Bezpečnostný prieskum, (bezpečnostný ďalej BP) je nástroj na poznanie bezpečnostnej situácie skúmanej entity.

Cieľom BP prieskumu je:

- preskúmanie bezpečnostných vlastností skúmanej entity,
- poznanie bezpečnostnej situácie,
- získanie informácii pre zvolenú metodiku analýzy bezpečnosti,
- vytvorenie modelu entity vo vzťahu k bezpečnostnej situácii,
- následná syntéza zo získaných poznatkov.

Výber metód bezpečnostného prieskumu a metód analýzy bezpečnosti závisí od účelu, cieľu bezpečnostného prieskumu:

Príklad cieľov BP prieskumu:

- vypracovanie bezpečnostného projektu objektu, entity,
- audit zavedenia bezpečnostného projektu do praxe,
- vypracovanie bezpečnostného projektu informačnej bezpečnosti podľa STN ISO/IEC 27001,
- audit systému riadenia informačnej bezpečnosti podľa STN ISO/IEC 27001,
- bezpečnostné posúdenie objektu podľa ČSN EN 50131-1-7 (za účelom montáže TP PKB),
- audit splnenia požiadaviek poisťovne za účelom uzatvorenia poistnej zmluvy (ČSN EN 50131-1, ČAP P131-7),
- audit vyžaduje zákon,
- audit vyžaduje zákazník, ako podmienku spolupráce.

Presná definícia cieľu bezpečnostného projektu je kľúčová pre výber metód bezpečnostného prieskumu, organizácie bezpečnostného prieskumu a výberu metódy bezpečnostnej analýzy.

1.2 Fáze bezpečnostného prieskumu

1.2.1 Predbežný prieskum

1.2.1.1 Definícia a účel predbežného prieskumu

Hlavným účelom predbežného BP prieskumu je oboznámenie sa z bezpečnostnou situáciou organizácie, ktorá je skúmaná. Cieľom je identifikovať problémové oblasti organizácie, pochopiť rozsah problému, identifikovať predstavy manažmentu o prínosoch bezpečnostného prieskumu tak, aby bolo možné určiť stratégiu a metódy bezpečnostného prieskumu.

Príprava na úvodný rozhovor s manažmentom organizácie, cieľ rozhovoru:

Cieľom úvodného rozhovoru s manažmentom organizácie je:

- identifikovať predstavy manažmentu o očakávaniach z výsledku bezpečnostného prieskumu,
- identifikovať problémové oblasti organizácie,
- identifikovať schopnosť kooperácie partnera,
- získať záväzok manažmentu o podpore činností bezpečnostného prieskumu,
- získať informácie o organizačnej štruktúre spoločnosti,
- získať kópie dokumentov bezpečnostných politík, bezpečnostných smerníc jednotlivých oblastí pre prípravnú fázu bezpečnostného prieskumu,
- získať informácie o roliach vedúcich pracovníkov v jednotlivých oblastiach o rozsahu ich zodpovedností,
- získať menný zoznam vedúcich pracovníkov a kontaktné údaje na nich.

Príprava na úvodný rozhovor je kľúčová pre úspešný priebeh a naplnenie cieľa rozhovoru.

Základné body prípravy:[1]

- naplánovať, získať vhodný termín a čas stretnutia,

[1] Poznámka:
Rozhovor by mal byť vykonaný s vrcholovým manažmentom organizácie, respektíve s vrcholovým manažérom, respektíve s osobou, ktorá má pridelené adekvátne kompetencie. Bezpečnostný špecialista musí byť na rozhovor pripravený a viesť ho stručne, zrozumiteľne, efektívne. Je potrebné vyhnúť sa nepodstatným podrobnostiam a poskytnúť len také informácie, ktoré sú potrebné pre rozhodovanie.

- vypracovať a zaslať manažmentu organizácie zoznam dokumentov potrebných pre prípravnú fázu bezpečnostného prieskumu (organizačná štruktúra spoločnosti, dokumenty bezpečnostných politík, bezpečnostné smernice jednotlivých oblastí a podobne),
- ozrejmiť ciele rozhovoru,
- určiť stratégiu a načrtnúť priebeh rozhovoru,
- pripraviť otázky pre manažment,
- pripraviť odpovede na možné otázky manažmentu,
- pripraviť dokumenty, ktoré by mal manažment podpísať, respektíve sa s nimi oboznámiť.

Rozhovor s manažmentom organizácie, vedenie, témy rozhovoru:

Je potrebné, aby manažment vymenoval bezpečnostné oblasti, ktoré považuje za problémové a stručne popísal históriu bezpečnostných incidentov problémových oblastí.

Ďalej je potrebné prediskutovať najmä očakávania o prínosoch bezpečnostného prieskumu s ohľadom na návrhy riešení pre problémové oblasti, za účelom vyhnutia sa prípadným nedorozumeniam, nepochopeniam, neprimeraným očakávaniam.

Schopnosť kooperovať, respektíve poskytnúť súčinnosť na výsledku bezpečnostného prieskumu je z hľadiska vykonania BP prieskumu kľúčová. Túto schopnosť je možné posúdiť počas rozhovoru a na základe obsahu zodpovedaných otázok manažmentom.

Ďalej je potrebné získať vyhlásenie manažmentu o podpore BP prieskumu v písomnej forme. Tento dokument by mal byť podpísaný najvyššou autoritou v organizácii. Obsahom tohto dokumentu by mal byť popis cieľov BP prieskumu, definícia podmienok kooperácie všetkých zamestnancov organizácie s prieskumným tímom. Dokument by mal autorizovať prístup ku všetkým dokumentom a informáciám, súvisiacich s predmetom bezpečnostného prieskumu. S týmto dokumentom by mali byť oboznámení vedúci pracovníci organizácie.[2] Ďalej je potrebné získať menný zoznam vedúcich pracovníkov a kontaktné údaje na nich.

[2] Bežnou praxou je aj určenie sprievodcu zo strany organizácie, ktorý sprevádza prieskumný tím počas prieskumu.

1.2.2 Analýza rizík zákazky

Analýza rizík zákazky je vykonávaná za účelom prehodnotenia schopnosti vlastnej organizácie naplniť ciele bezpečnostného prieskumu z pohľadu vlastnej odbornosti, rozsahu činností a časového rámca v ktorom má byť prieskum realizovaný. Ďalej je posudzovaná primeranosť očakávaní manažmentu o prínosoch bezpečnostného prieskumu a schopnosť kooperácie skúmanej organizácie. Analýza rizík zákazky vychádza z informácii získaných pri predbežnom bezpečnostnom prieskume.

1.2.3 Prípravná fáza bezpečnostného prieskumu

1.2.3.1 Presné vytýčenie cieľa bezpečnostného prieskumu zámer

Presné vytýčenie cieľa bezpečnostného prieskumu je kľúčové z pohľadu stratégie ďalších činností. Výber metód bezpečnostného prieskumu a metód analýzy bezpečnosti závisí od účelu, cieľu bezpečnostného prieskumu:

Obecným cieľom BP prieskumu je:

- preskúmanie bezpečnostných vlastností skúmanej entity,
- poznanie bezpečnostnej situácie,
- získanie informácii pre zvolenú metodiku analýzy bezpečnosti,
- vytvorenie modelu entity vo vzťahu k bezpečnostnej situácii,
- následná syntéza zo získaných poznatkov.

Presným vytýčením cieľa môže byť napríklad bezpečnostné posúdenie objektu podľa ČSN EN 50131-1-7, prípadne BP prieskum pre systém riadenia informačnej bezpečnosti podľa STN ISO/IEC 27001.

1.2.3.2 Určenie stratégie bezpečnostného prieskumu

Stratégia vychádza z cieľa, ktorý má BP prieskum dosiahnuť, rozsahu poznaného problému, ktorý sa má riešiť a dostupných zdrojov personálneho, technického a ekonomického charakteru.

Určuje základný rámec riešenia problému z hľadiska:

- postupov a úloh,
- časového rámca,
- vymedzených zdrojov,

- zvolených metód BP prieskumu,
- komunikačnej stratégie zo so zákazníkom,
- stratégie a metód získavania informácii v prieskume,
- zložitosti organizačnej štruktúry organizácie.

1.2.3.3 Výber metodiky bezpečnostného prieskumu

Metodikou rozumieme presne stanovenú logickú postupnosť činností zameranú na dosiahnutie stanovených cieľov s pomocou týchto metód vedecko-výskumnej činnosti. Vypracovanie metodiky má veľký praktický význam. Závisí na tom kvalita záverov a doporučení a včasnosť získania týchto záverov a doporučení za predpokladu, že realizátori budú zabezpečení po stránke informačnej. Metodika výskumnej činnosti logicky vyplýva z metodiky analýzy. Analýza je metódou poznania reálnej skutočnosti. (1)

Výber metód určuje stratégia bezpečnostného prieskumu, ktorá závisí od cieľa bezpečnostného prieskumu, vlastností skúmanej entity a bezpečnostnej situácie, vybranej metódy analýzy bezpečnosti.

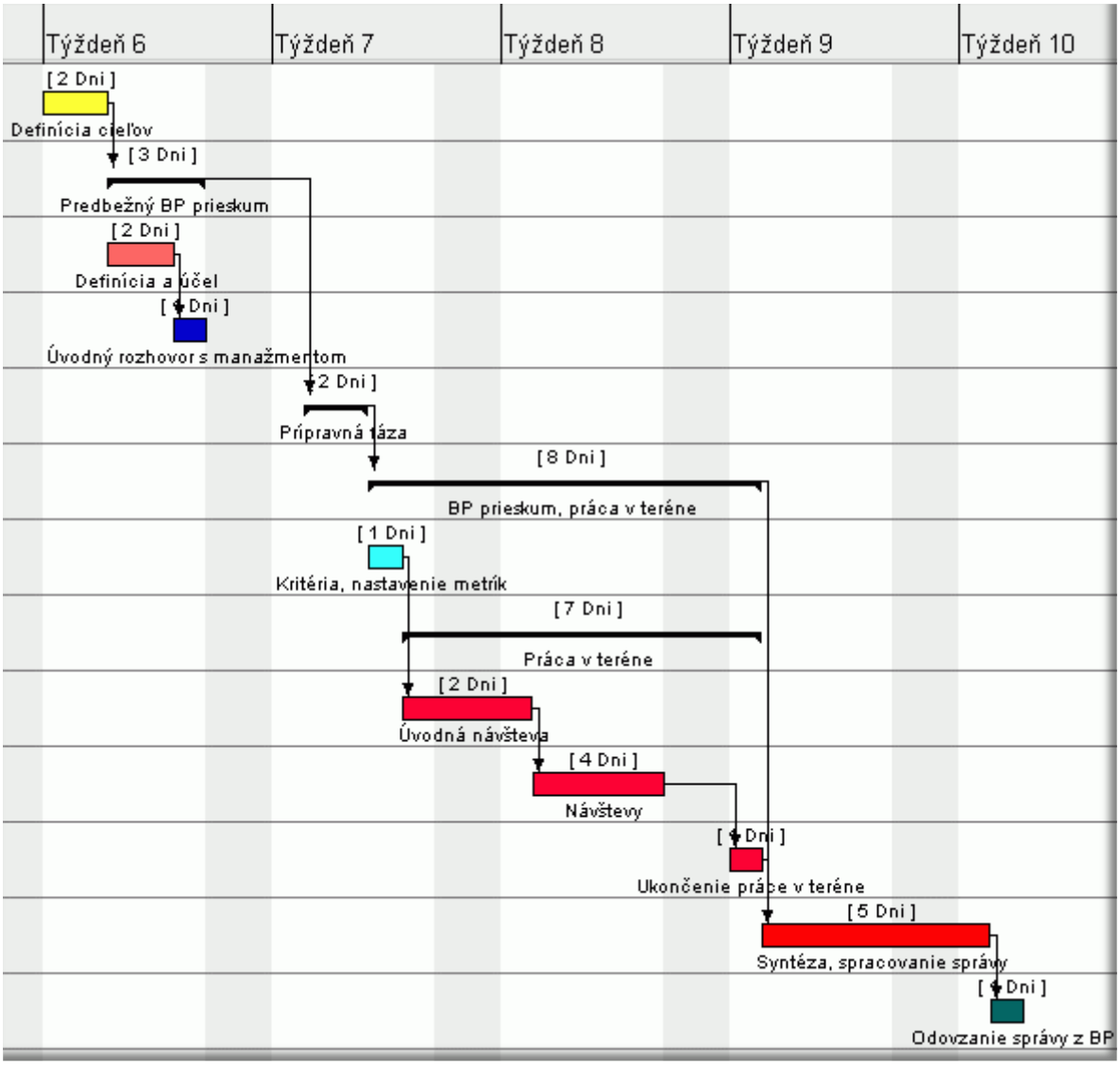
1.2.3.4 Plánovanie projekt manažment

Základný rámec pre projekt manažment určuje stratégia bezpečnostného prieskumu a vybraná metodika. Výstupom plánovacej činnosti je plán, ktorý určuje spôsoby postupnosť úloh dosiahnutia cieľov BP prieskumu v určenom časovom rámci a s využitím pridelených zdrojov. Obsahom plánu je podrobný popis úloh ich časovú následnosť a vzťahy medzi jednotlivými úlohami, kooperáciu členov tímu. Obsahuje popis etáp bezpečnostného prieskumu, jednotlivé kontrolné body procesu.

Charakteristické rysy projektov:

Cieľ projektu: projekty majú trojrozmerný cieľ, čo znamená naplnenie cieľa projektu v definovanom časovom rámci a nákladoch (spotrebovaných zdrojoch). Úspešné riadenie projektu vyžaduje, aby tieto tri podmienky boli merateľné (t.j. konkrétne, overiteľné a dosiahnuteľné). (2)

Jedinečnosť projektu: každý projekt je jedinečný, pretože sa vykonáva len raz, je dočasný a takmer vždy na ňom pracuje iná skupina ľudí.



Obrázok 1: plán BP prieskumu Ganttov diagram

Vyčlenené zdroje pre projekt: projekty sú realizované prostredníctvom ľudských a materiálnych zdrojov. Nad mnohými z požadovaných zdrojov má projekt manažér len minimálnu kontrolu.

Proces riadenia projektov: riadenie projektov pozostáva z piatich odlišných manažérskych činností:

- **definícia projektových cieľov,**
- **plánovanie:** naplnenie cieľu projektu v určenom čase a v určených nákladoch t.j. špecifikácia vykonania, časový plán a finančný rozpočet,
- **vedenie ľudí:** riadenie ľudských zdrojov aby vykonali požadované úlohy efektívne a včas a v požadovanej definícii úloh,

- **monitorovanie:** kontrola stavu a postupu projektových prác, aby sa včas zistili odchýlky od plánu a mohlo sa včas pristúpiť k ich korekcii,
- **ukončenie:** overenie, že hotová úloha zodpovedá aktuálnej definícii toho, čo sa malo urobiť a uzatvorenie nedokončených prác.

1.2.3.5 Výber ľudí

Bezpečnostný prieskum z hľadiska systematizácie priemyslu komerčnej bezpečnosti je činnosť analytických útvarov. Bezpečnostný prieskum vykonávajú bezpečnostní špecialisti. Je to jedna z najnáročnejších činností v priemysle komerčnej bezpečnosti, ktorá je náročná na znalosti, skúsenosti, intuíciu a vyžaduje systematický prístup. Vedúci tímu musí mať dostatočné skúsenosti z realizáciou bezpečnostných prieskumov. Zloženie tímu závisí od cieľu bezpečnostného projektu, problematiky ktorá má byť riešená a organizačnej štruktúry skúmanej organizácie. Na základe štruktúry problému sú do tímu vyberaní konzultanti zo zameraním na jednotlivé bezpečnostné oblasti.

1.2.3.6 Štúdium dostupných a získanie ďalších informácií o organizácii

V procese BP prieskumu sú využívané informácie, ktoré sú v dokumentoch zafixované rôznym spôsobom.

Dokument: ľubovoľný materiálny nosič informácii v ktorom sú v ľubovoľnom jazyku zafixované informácie potrebné k dosiahnutiu cieľov.

Podľa spôsobu fixácie dokumenty delíme na:

- písomné dokumenty (rukopisy, strojopisy, počítačové výstupné zostavy),
- grafické dokumenty (mapy, obrázky, fotodokumentácia, video dokumentácia, iné nosiče),
- zvukové dokumenty (CD, DVD, MGF pásky, obecne iné nosiče dát),
- špeciálne dokumenty informačných technológií.

Dokumenty delíme ďalej na:

- Manažérsko-organizačné: (plány, rozkazy, pokyny, smernice atď.). Cirkulujú v organizácii priamymi komunikačnými kanálmi od subjektu k objektu riadenia, spravidla pomocou informačných médií (siete, nosiče dát).
- Informačné: cirkulujú od objektov k subjektu riadenia a naopak. (1)

Pokiaľ je možné je potrebné získať kópie dokumentov organizácie:

- Základnú zriaďovateľskú listinu organizácie (spoločenská zmluva, zriaďovateľská listina organizácii zriaďovaných štátom, alebo samosprávou).
- Základný dokument bezpečnostnej politiky organizácie a ďalšie bezpečnostné politiky jednotlivých bezpečnostných oblastí ak existujú (napríklad bezpečnostná politika informačnej bezpečnosti.
- Dokumentácia k zavedeným procesom, ktoré majú vzťah k bezpečnosti. Napríklad periodické školenia povedomia o bezpečnosti, preskúšavanie personálu, procesy bezpečnosti ľudských zdrojov.
- Havarijné plány.
- Prevádzkový poriadok areálu, budov.
- Jednotlivé smernice bezpečnostných oblastí:
    - pre výkon strážnej služby,
    - smernice pre kontrolu vstupu, kľúčový poriadok,
    - požiarne smernice,
    - smernice pre prácu s informačnými systémami,
    - smernice pre správu informačných systémov.
- Revízie systémov budov: požiarne, elektroinštalácie, vzduchotechniky.
- Organizačný poriadok, štruktúra, mená, rozsah kompetentností a role zamestnancov.

Ak organizácia neposkytne kópie týchto dokumentov (z bezpečnostných dôvodov ochrany informácii), tak je potrebné si vyžiadať tieto dokumenty ku štúdiu v mieste organizácie.

1.2.3.7 Oznámenie návštevy

Cieľom oznámenia návštevy je umožniť organizácii aby sa pripravila na bezpečnostný prieskum a zároveň poskytuje informácie o procese bezpečnostného prieskumu:

- dátum a čas,
- cieľ bezpečnostného prieskumu,
- mená členov tímu,
- spôsob identifikácie členov tímu (nahlásenie osobných údajov členov tímu zaslanie fotografií pre identifikáciu osôb, na mieste prieskumu overenie identity osôb napríklad predložením občianskeho preukazu a porovnaním zo zaslanými fotografiami),

- požadované dokumenty,
- vybrané metódy zberu informácii,
- vybrané technické prostriedky zberu informácii,
- preverovaný útvar,
- hrubý časový rozvrh,
- požadovaná prítomnosť osôb.

Je potrebné zo strany skúmanej organizácie zabezpečiť sprievodcu. Oznámenie návštevy musí byť vykonané písomne a v dostatočnom časovom predstihu.

1.2.3.8 Príprava pre prácu v teréne

Príprava pozostáva z:

- z overenia, či bolo akceptované oznámenie o návšteve zo strany manažmentu organizácie,
- prípravy formulárov, dotazníkov a otázok pre metodiku bezpečnostného prieskumu,
- prípravy technických prostriedkov bezpečnostného prieskumu ak budú použité.

Porada, príprava pracovného tímu pozostáva z bodov:

- oboznámenie členov tímu s cieľom a účelom BP prieskumu,
- oboznámenie členov tímu zo stratégiou BP prieskumu,
- s metodikou BP prieskumu,
- s plánom a časovým rozvrhom BP prieskumu,
- oboznámenie členov tímu s informáciami získanými predbežným BP prieskumom,
- oboznámenie členov tímu s metodikou BP prieskumu,
- určenie rolí členov tímu a určenie bezpečnostných oblastí, ktoré budú skúmať,
- oboznámenie členov tímu s pravidlami vyplňovania tlačív a formulárov,
- preskúšania členov tímu,
- preverenia úplnosti všetkých potrebných dokumentov a technických prostriedkov.

1.2.4 Bezpečnostný prieskum: práca v teréne

Z hľadiska spotreby času pre vypracovanie bezpečnostného prieskumu je možné percentuálne čas rozdeliť na :

- 50 percent času je potrebných pre prácu v teréne,
- 50 percent času je potrebných pre plánovanie prieskumu, analýzu a následnú syntézu informácii.

Práca v teréne pozostáva zo zbieraní informácii, vytváraní záznamov a preskúmavaní procesov. Má zásadný vplyv na výsledok celého procesu bezpečnostného prieskumu. (1) Cieľom je získať kvalitné informácie v určenom časovom rámci. Výber metód zberu informácii v teréne závisí od metódy analýzy bezpečnosti, ktorá bude použitá.

Predmetom skúmania sú bezpečnostné:

- politiky,
- technické opatrenia,
- organizačné opatrenia,
- personálne opatrenia,
- bezpečnostné procedúry,
- ostatné procesy a operácie.

Ďalej je potrebne identifikovať kritické faktory, ktoré majú vplyv na bezpečnosť. (1)

Pre vykonanie práce v teréne je potrebné spracovať projektový plán, ktorý určuje:

- skúmanú entitu, alebo časť entity,
- miesto skúmania,
- zdroje pre skúmanie,
- časový rámec skúmania.

Pre samotné získavanie informácii je potrebné mať pripravené:

- formuláre pre metódu pozorovania, ktoré sú vyplňované počas práce v teréne,
- formulované otázky pre metódu rozhovoru, štruktúrované podľa bezpečnostných oblastí.

Tieto formuláre sú dôležitou pomôckou pre zabezpečenie presnosti, včasnosti a úplnosti zberu informácií.

Tieto formuláre je možné mať pripravené:

v papierovej forme:

- výhody: rýchly zápis počas rozhovoru, nestráca sa kontakt s respondentom,

- nevýhody: z hľadiska automatizovaného spracovania nevhodné.

v elektronickej forme:

- výhody: informácie sú v štruktúrovanej forme pre ďalšie automatizované spracovanie, je možné zabezpečiť vyššiu kvalitu zadávaných informácii,
- nevýhody: dlhšie trvajúci náročnejší zápis informácií, narušuje plynulosť rozhovoru, stráca sa kontakt s respondentom.

Impl. BP opatrenia podľa STN ISO 27002

BP kategória	Bezpečnostné opatrenie	Otázka - zistenie stavu impl.	Pozn. pre hodnotiteľa
5.1 Politika informačnej bezpečnosti	5.1.1 Dokument politiky informačnej bezpečnosti	Existuje bezpečnostná politika informačnej bezpečnosti, je schválená menežmentom organizácie?	Overuje sa fyzická existencia dokumentu. Dokument musí byť schválený menežmentom organizácie. Zapisuje
5.1 Politika informačnej bezpečnosti	5.1.1 Dokument politiky informačnej bezpečnosti	Sú v bezpečnostnej politike určené bezpečnostné ciele?	Overuje sa obsah BP.
5.1 Politika informačnej bezpečnosti	5.1.2 Preskúmanie politiky informačnej bezpečnosti	Sú určené metódy a intervaly preskúmavania bezpečnostnej politiky a postupy pri výskyte významných zmien?	Zisťuje sa existencia schválených metódy preskúmavania bezpečnostnej politiky.
5.1 Politika informačnej bezpečnosti	5.1.1 Dokument politiky informačnej bezpečnosti	Sú určené spôsoby ich vyhodnocovania alebo dosahovania bezpečnostných cieľov? Ak áno, ako?	Overuje sa obsah BP.
5.1 Politika informačnej bezpečnosti	5.1.1 Dokument politiky informačnej bezpečnosti	Obsahuje bezpečnostná politika podporu vedenia?	Overuje sa existencia vyhlásenia o podpore vedenia resp. podpis vedúceho pracovníka (v rámci schvaľovacieho

Obrázok 2: ukážka formuláru s pripravenými otázkami pre BP prieskum

1.2.4.1 Kritéria merania: nastavenie metrík

Práca v teréne je z veľkej časti meranie a ohodnocovanie efektívnosti prijatých bezpečnostných opatrení a procesov. Ak majú mať tieto merania a ohodnocovania zmysel,

ich základom musia byť objektívne štandardy (metriky) merania. Metriky musia byť v dostatočnej miere akceptovateľné voči predmetu merania a porovnávania. Každá časť bezpečnostného prieskumu musí byť vykonaná s ohľadom na zvolené metriky.[3] Metriky je potrebné nastaviť podľa existujúcich štandardov a noriem, alebo pravidiel dobrej praxe. Ak metriky neexistujú, tak ich konzultant musí definovať vzhľadom na problematiku skúmanej entity. Takto definovaná metrika musí brať do úvahy aspekty spoľahlivosti, kvality, ceny a vykonateľnosti meraní. (1)

1.2.4.2 Ukončenie práce v teréne

V tejto fáze je potrebné preveriť, kontrolné zoznamy, formuláre, či boli získané všetky informácie pre syntézu z bezpečnostného prieskumu.

1.2.5 Syntéza

Obecná syntéza je metóda, ktorá využíva obecných záverov analytickej činnosti (rozboru situácie) pre vykonanie optimálneho a efektívneho zloženia získaných informácií do nového celku na základe ktorého je prijaté riadiace rozhodnutie na kvalitatívne vyššom základe. Ide o kvalitatívne vyšší rozhodovací výstup informácií pre vrcholový manažment. Syntéza je dôležitá pre myšlienkový sled manažmentu postupujúci od najjednoduchších pojmov, alebo faktov (javov, udalostí) ku zložitejším. Z hľadiska riadenia činnosti PKB ide o nadväzovanie a nachádzanie súvislostí. Syntéza je vlastne zjednotenie jednotlivých častí (javov, skutkov, udalostí) vydelených analýzou.

Analogická syntéza je metóda pri ktorej použitím systémovej analýzy a obecnej syntézy dosahujeme vyššiu úroveň znalostí o faktoch. Použitím analogickej syntézy hľadáme správny vzťah medzi podobnosťami a totožnosťami. Je hlavne používaná pri modelovaní teóriou podobnosti a musí ukazovať nie len podobnosť, ale aj rozdielnosť objektov, javov, udalostí. Pomocou analogickej syntézy vykonávame modelovanie (udalostí, činností, javov). Ide o reprodukciu vlastností skúmaného objektu (udalostí, činností, skutkov, javov) na analogickom objekte zostrojenom podľa určitých pravidiel. Tento analogický objekt nazývame modelom. (4)

---

[3] Ak bezpečnostný špecialista vykonáva bezpečnostný prieskum bez definície metrík, produkuje iba subjektívne pozorovania, nie objektívne výstupy založené na štandardoch a dobrej praxi.

1.2.5.1 Štruktúra správy z bezpečnostného prieskumu

1. Účel, cieľ bezpečnostného prieskumu: mal by zahrňovať účel, dôvod vykonania prieskumu.

2. Pôsobnosť, zameranie: stručne popísať rozsah, hĺbku skúmania. To znamená do akej hĺbky boli bezpečnostné oblasti skúmané, respektíve do akých detailov. [4]

- Predmet skúmania, postupy, popis vybraných metód bezpečnostného prieskumu.
- Ktorí ľudia podali informácie, ich pozícia, ktoré priestory a časti entity boli skúmané, časový rámec v ktorom bol prieskum vykonaná.
- Kategórie skúmaných dokumentov.
- Skúmané procesy.

3. Zistenia:

Zistenia, ktoré priamo súvisia s účelom a cieľom BP prieskumu. Napríklad správa z bezpečnostnej oblasti fyzickej bezpečnosti by mala vymenovávať zistené nedostatky v opatreniach fyzickej bezpečnosti vo vzťahu k chránenému aktívu. Správa by ďalej mala obsahovať:

Popis organizácie jej ciele jej činnosti: zameranie organizácie, organizačná štruktúra, počet zamestnancov, procesy súvisiace s bezpečnosťou.

Popisy budov, prostredia, operácií, produktov, alebo služieb a rozvrhy.

Popis stavu fyzickej bezpečnosti: popis prijatých organizačných, personálnych, technických opatrení, ohodnotenie efektívnosti týchto opatrení.

Napríklad:

- Organizačné opatrenia, popis smerníc: strážnej služby, prevádzkový poriadok budovy, areálu, popis režimu vstupu, pracovný poriadok a podobne.
- Personálne opatrenia: popis organizačnej štruktúry riadenia bezpečnosti, priradenie zodpovedností za výkon konkrétnym osobám, disciplinárny poriadok a pod..
- Technické opatrenia: popis budov ich konštrukčných vlastností, popis inštalovaných technických prvkov priemyslu komerčnej bezpečnosti.

[4] Prieskum musí brať do úvahy aspekty primeranosti a nákladov. Tieto aspekty určuje účel bezpečnostného prieskumu.

Popis metód a procedúr interných kontrolných mechanizmov:

Napríklad:

- Kontrola skladu a zoznamov materiálu, frekvencia inventúr majetku, spôsob vykonania inventúr, spôsob overenia inventúr, ktoré osoby vykonávajú inventúry. (1)

Informačné systémy a záznamy: vymenovanie typov informácií, popis prijatých bezpečnostných opatrení pre zabezpečenie informácií.

Havarijné plánovanie: popis havarijných plánov, rozsah plánovania.

Popis jednotlivých fáz:

- príprava na mimoriadne situácie,
- činnosť počas mimoriadnych udalostí (reakcia),
- obnova po mimoriadnych udalostiach,
- história incidentov, mimoriadnych udalostí.

4.Závery:

Rozvinúť merania, z časti 3: zistenia. Identifikácia špecifických zraniteľností, hodnotenie podľa miery rizika a hodnoty dopadov na chránené aktíva.

5. Návrhy opatrení:

Konkrétne návrhy opatrení podľa konkrétnych bezpečnostných oblastí.[5]

[5] Napríklad bezpečnostné oblasti pre riadenie informačnej bezpečnosti:

- bezpečnostná politika,
- organizácia informačnej bezpečnosti,
- riadenie aktív,
- bezpečnosť ľudských zdrojov,
- fyzická bezpečnosť a bezpečnosť prostredia,
- riadenie komunikácie a prevádzky,
- riadenie prístupu,
- akvizícia vývoj a údržba informačných systémov,
- riadenie incidentov informačnej bezpečnosti,
- riadenie kontinuity činnosti,
- súlad.

1.2.5.2 Zásady pre správne spracovanie dokumentov priemyslu komerčnej bezpečnosti

Obecné požiadavky kladené na dokumenty PKB:

- všetky dokumenty v PKB majú byť apolitické,
- musia byť v poriadku po právnej stránke (ich obsah a spôsob získania musí byť v súlade zo zákonmi),
- obsah dokumentov musí byť objektívny (a musí zodpovedať bezpečnostnej politike a etike bezpečnostnej práce),
- obsah dokumentov má rešpektovať chránené záujmy ako vnútropodnikové, tak aj záujmy zákazníkov (utajenie, ochrana informácií, ochrana know-how, ochrana zákazníkov). (1)

Požiadavky na štruktúru dokumentov:

- dokumenty majú mať vypovedaciu schopnosť,
- majú byť stručné a výstižné,
- cieľavedome spracované (názov dokumentu, text, anotácia, spôsob využitia, určenie, počet výtlačkov, kópií, zabezpečenie ochrany nosičov dát).

Dokumenty sa spracovávajú pre niekoho, preto je dôležitá anotácia k orientácii v probléme. Majú tu byť vyjadrené technologické pravidlá spracovania, vecnosť, presnosť, úplnosť, zrozumiteľnosť, stručnosť.

Normatívne regulovanie procesu dokumentácie bezpečnostnej činnosti: niektoré dokumenty je potrebné dlhodobo uchovávať, za účelom doloženia svojej činnosti[6] a to hlavne jej bezchybnosť, správnosť, zákonnosť, legálnosť.

Štandardizácia, unifikácia, formalizácia bezpečnostných dokumentov: tu je doporučené spracovanie a využívanie štandardných, alebo unifikovaných dokumentov.

1.2.5.3 Zásady pre správne spracovanie správy z bezpečnostného prieskumu

Hlavné kritéria: presnosť, zrozumiteľnosť, stručnosť, včasnosť, vlastný názor (stanovisko).

---

[6] Napríklad doloženie informácií z BP prieskumu, ktoré boli vytvorené v určitom mieste a čase, ktoré boli podkladom pre analýzu bezpečnosti, respektíve vytvorenie modelu bezpečnostnej situácie.

Presnosť: Správa o BP prieskume musí dokumentovaná na základe faktov, logických záverov a nastavených metrík, musí byť podložená faktami, informáciami z práce v teréne v písomnej forme. Informácie, použité fakty musia byť overené. V prípade, že je nevyhnutné v správe použiť informácie a fakty, ktoré neboli osobne získané je potrebné identifikovať zdroj týchto informácii. Informácie musia byť odosobnené. Respektíve autor sa musí vyhnúť subjektívnemu pohľadu. Fakty je potrebné prezentovať v správnom svetle a v súvislostiach, nie samostatne, správa musí byť vyvážená, presná musí popisovať reálny stav, zo správnej perspektívy. (1)

Zrozumiteľnosť:

Správa je určená pre manažment organizácie, nie pre odbornú verejnosť. Informácie musia byť v správe podané tak, aby jej manažment organizácie porozumel. Text musí byť správne štruktúrovaný, slabá štruktúra textu je prekážkou zrozumiteľnosti. Vety musia byť formulované zrozumiteľne, výstižne je dôležité nepoužívať odborné termíny, odkazy na odbornú literatúru a odborné skratky. Ak je odborné termíny potrebné použiť je potrebné ich definovať v definícii pojmov. Informácie je potrebné podávať vždy v súvislostiach. Ak je navrhovaná procedúra je potrebné popísať terajší stav, vysvetliť dôvody, prečo je procedúra navrhovaná a vysvetliť spôsob jej zavedenia do praxe a očakávaný stav po jej správnom zavedení. Pre vysvetlenie je potrebné používať nástroje, ako sú vývojové diagramy, myšlienkové mapy, rozvrhy, vzorky, ukážky, grafy, obrázky, videá.

Stručnosť:

Stručnosť znamená elimináciu toho, čo je nepodstatné. Stručnosť neznamená stratu podstatných informácii. Tiež to neznamená, že správa bude obsahovo krátka. Stručnosť znamená odstránenie retundatných, alebo zbytočných informácii, ktoré nesúvisia s predmetom správy.

Včasnosť:

Informácie z bezpečnostného prieskumu je potrebné spracovať v definovanom časovom rámci vzhľadom na skutočnosť, že bezpečnostná situácia sa časom vyvíja, vyvíjajú sa hrozby, menia sa pravdepodobnosti ich naplnenia voči aktívu, mení sa úroveň zavedených bezpečnostných opatrení, mení sa prostredie.

Zo zväčšujúcim sa časovým intervalom medzi začiatkom prieskumu a ukončením prieskumu hodnota informácii klesá po prekročení tohto rámca sú informáciu pre analýzu

bezpečnosti nepoužiteľné. Časový rámec sa určuje na základe zložitosti organizačnej štruktúry organizácie, rozsahu problematiky a vybranej metodiky analýzy rizík.

Zistenia:

Zistenia sú produktom práce v teréne. Pri príprave prezentácie zistenia je potrebné odpovedať na otázky:

- V čom je problém?
- Ktorí ľudia, procedúry sú súčasťou problému?
- Ktorí ľudia, procedúry by mali problém riešiť?
- Prečo problém neriešili, ak o ňom vedia?
- Čo sa stane, keď sa neurobí nič?
- Ako môže dôjsť k mimoriadnej situácii?
- Čo by sa s problémom dalo robiť?
- Kto je za to zodpovedný za spôsobenie problému?
- Kto je zodpovedný za riešenie problému?

Názor a záver

Vyjadrenie vlastného názoru k úrovni bezpečnosti jednotlivých bezpečnostných oblasti. Vlastný je profesionálne posúdenie jednotlivých bezpečnostných oblastí podložené faktami. Má poukázať na problém a navrhnúť možné riešenie.

2 PSYCHOLOGICKÉ A PSYCHOANALYTICKÉ ASPEKTY POSTUPU

2.1 Komunikácia

Komunikácia je jedným zo základných prostriedkov pre získavanie informácii.

2.1.1 Sociálna komunikácia

Je poskytnutie a zdieľanie informácii medzi dvomi a viacerými ľuďmi, ktoré prebieha na dvoch úrovniach a to na úrovni verbálnej a na úrovni neverbálnej. Komunikácia pozostáva z vysielania informácií a ich príjmu. Sociálna komunikácia neprebieha nikdy len jedným smerom, od jedného človeka ku druhému, ale vždy obojstranne, alebo viacstranne podľa toho, koľko ľudí sa práve nachádza v spoločnom priestore. Sociálna komunikácia určuje, aký bude vzťah medzi komunikujúcimi ľuďmi. (3)

2.1.2 Hlavné príčiny nedorozumení v komunikácii

Hlavnými príčinami nedorozumení sú:

- Nezrozumiteľné, zastrené vyjadrenie myšlienky.
- Používanie slov a formulácii, ktorým partner nerozumie (príliš odborné, alebo slangové slová, prílišný popis detailov).
- Používanie mnohovýznamových slov, alebo neurčitých výrazov.
- Nejasné a nejednoznačné formulovanie myšlienok, ktoré pripúšťajú ľubovoľný voľný výklad v prospech, alebo v neprospech počúvajúceho. Táto forma budí neistotu a dáva príležitosť k vlastnému domýšľaniu poskytovaných informácií.
- Nepozornosť, alebo nezáujem jednej zo strán, kedy často dôjde k úplnému skresleniu informácie.
- Citové predsudky príjemcu k poskytnutej informácii.
- Odmietavé predsudky, alebo nekritické postoje jednej zo strán ku druhej.
- Rozpor medzi verbálnym obsahom a neverbálnou informáciou. (3)

2.1.3 Aktívne načúvanie

Komunikácia nie je len poskytovanie a príjem informácii, alebo pasívny príjem zvukov, ale je to aktívna činnosť:

- parafrázovania,
- zapojovania viacerých zmyslov,
- kladenia doplňujúcich otázok,
- vyžadovania a poskytovania spätnej väzby,
- rekapitulovania počutého,
- schopnosť počuť fakty,
- schopnosť „počuť“ emócie, ktoré druhý prežíva pri poskytovaní správy.

Existuje veľa prekážok, ktoré ovplyvňujú proces načúvania. (3)

Prekážky načúvania:

- koncentrácia problémov: počúvanie vyžaduje 100 % koncentráciu,
- načúvanie a premýšľanie nejdú spolu dokopy (duševné preťaženie),
- načúvanie je ťažké, v prípade nesúhlasu s druhou osobou,
- nadmerné emócie,
- selektívne načúvanie (ľudia počujú, čo chcú počuť).

2.1.4 Technika kladenia otázok

Na to, aby sa partner rozhovoril je potrebné použiť vhodnú otázku. Na začiatku je vhodné položiť otvorenú otázku na ktorú partner odpovedá voľne väčšinou dlhšou výpoveďou. Ak je potrebné priebeh rozhovoru urýchliť, tak je možné položiť niekoľko uzavretých otázok, na ktoré partner odpovedá áno, nie. Túto formu uzavretých otázok je potrebné použiť opatrne, aby sa z rozhovoru nestal výsluch.

2.1.4.1 Otvorené otázky

Otvorené otázky začínajú opytovacími zámenami: čo, kto, kedy, ako, aký, prečo a pod. Otvorená otázka stimuluje myslenie a necháva priestor pre mnohé odpovede. Odpoveď poskytuje mnoho informácii.

2.1.4.2 Uzavreté otázky

Uzavretá otázka môže byť zodpovedaná iba áno, nie, neviem. Uzatvorené otázky majú veľkú hodnotu v prípade kontroly informácii behom komunikácie, lebo odpovede sú na nich jasné a stručné. Uzavreté otázky sa začínajú slovesom.

2.1.4.3 Výberové / alternatívne otázky

Otázky typu buď/alebo nepriamo nútia odpovedajúceho k výberu medzi obmedzeným počtom ponúknutých odpovedí. Otázky ponúkajú alternatívu, sú vhodné pre použitie pri upresňovaní informácii.

2.1.4.4 Riadiace otázky

Riadiace otázky nútia odpovedajúcu osobu odpovedať tak, ako chce ten, kto otázku položil. Obvykle sa v otázke vyskytujú slová ako: predpokladajme, nemyslíte. Pýtajúca sa osoba uvádza svoju hypotézu v otázke.

2.1.5 Techniky zvládania konfliktov a agresie

Konflikt je destabilizujúci aspekt systému (môže spôsobiť podstatnú zmenu jeho stavu, alebo zánik.)

Delenie konfliktov:

- extrapersonálny: prebieha mimo ľudskú pôsobnosť,
- intrapersonálny: prebieha vo vnútri ľudského indivídua,
- interpersonálny: prebieha medzi dvomi indivíduami.

2.1.5.1 Intrapersonálne konflikty

Charakteristické rysy: rozhodovanie medzi minimálne dvomi motívmi, ktoré sú rovnako závažné, ale navzájom sa vylučujú. Sprievodné javy: váhanie, kolísanie, bezradnosť, oscilácia okolo stredu.

2.1.5.2 Interpersonálne konflikty

Charakteristické rysy: stret predstáv, názorov, postojov, záujmov medzi ľuďmi (skupinami ľudí). Sprievodné javy: vznik záporných emócii, narušenie komunikácie, narušenie medziľudských vzťahov, narušenie stability systému.

Typy týchto konfliktov:

- spor: s konkrétnymi spôsobmi vecného riešenia sa identifikujú určité osoby, alebo skupiny osôb: personifikovaný problém,
- problém: nedochádza k identifikácii osôb s konkrétnymi spôsobmi vecného riešenia: depersonifikovaný spor.

Existencia konfliktov je legitímna:

- každý človek má právo slobodne a originálne myslieť a hlásať svoje myšlienky,
- názory a záujmy jednotlivých ľudí sa môžu líšiť,
- tieto odlišnosti stimulujú ďalší vývoj,
- úplne sa zbaviť konfliktov je nemožné.

Konflikty sú užitočné:

- neexistencia konfliktov vedie k stagnácii systému a jeho degradácii,
- neriešenie konfliktov vedie k destabilizácii a revolučnej zmene systému,
- riešenie konfliktov stabilizuje systém a je predpokladom plynulej evolúcie,
- kto nie je trvalo schopný riešiť konflikty, nie je schopný sa adaptovať na zmeny a riskuje svoj zánik. (3)

2.1.5.3 Možné riešenia konfliktov

- **Pasivita:** spoliehanie sa na spontánne, prípadne náhodné riešenie konfliktu.
- **Losovanie:** pokročilejší spôsob náhodného riešenia. Účastníci konfliktu však už rozhodujú, ako a kedy sa náhoda prejaví.
- **Násilie:** od slovnej urážky, až po tretiu svetovú vojnu. Bez pravidiel: bitka, s pravidlami: súboj.
- **Delegácia:** účastníci delegujú právo rozhodnúť na vonkajšiu autoritu.
- **Vyjednávanie:** riešenie konfliktu diskusiou. Je možné očakávať výsledok s ktorým bude spokojná väčšina, možno aj všetci účastníci.

Riešenie konfliktov[7] vyjednávaním:

Sú možné tri úrovne diskusie:

---

[7] Praktické rady pre riešenie konfliktov:
- zahájiť riešenie už pri prvých príznakoch,
- oddeliť od seba jednotlivé strany a vylúčiť násilné riešenie konfliktu,
- pokiaľ to ide, previesť spor na problém,
- obmedziť počet účastníkov konfliktu,
- bezodkladne zahájiť vyjednávanie,
- ponúknuť stranám možnosť dialógu,
- motivovať jednotlivé strany k dosiahnutiu pozitívnych výsledkov vyjednávania,
- akceptovať závery vyjednávania.

- **Monológ:** tam kde rozhoduje autorita. Rozhodujúce informácie vo forme príkazov prúdia jedným smerom, opačný tok nie je reflektovaný.
- **Dialóg:** rovnoprávna výmena informácii a rovnoprávne navrhovanie riešenia.
- **Trialóg:** zapojenie tretieho, neutrálneho prvku do diskusie. Je vhodný tam, kde sa účastníci diskusie chcú, ale nevedia sa dohodnúť. Tretia strana vystupuje v roli katalyzátoru.

Štyri fáze vyjednávania:

- vyjednávanie (spor riešený dialógom),
- mediácia (spor riešený trialógom),
- prejednávanie (problém, riešený dialógom),
- facilitácia (problém riešený trialógom).

2.2 Profesiografia, výber pracovníkov pre bezpečnostný prieskum

Profesiografia je popis činností sa stanovanie somatických i psychických požiadaviek pre určitú pracovnú profesiu. Bývajú uvedené podmienky, za ktorých sa dané odborné práce konajú. Na vypracovanie **profesiogramu**[8] sa preto zúčastňuje celá rada odborníkov.

---

[8] Príklad profesiogramu, ktorý vypracovala:
ENISA - European Network and Information Security Agency.

Funkcia: pracovník pre CSIRT Computer Security Incident Response Team – Tím pre reakciu na bezpečnostné incidenty počítačov.
Stručný prehľad najdôležitejších schopností technických odborníkov pre CSIRT.
Body opisu práce hlavných technických pracovníkov:
Osobné schopnosti

- Flexibilný, tvorivý a s dobrým zmyslom pre tím.
- Dobré analytické schopnosti.
- Schopnosť vysvetliť zložité technické otázky jednoduchými slovami.
- Dobrý cit pre dôvernosť a pre prácu na procedurálnych otázkach.
- Dobré organizačné schopnosti.
- Odolnosť voči stresu.
- Dobré schopnosti komunikácie a písania.
- Nezaujatý a ochotný učiť sa.

Technické schopnosti

- Široké znalosti technológie Internetu a protokolov.
- Znalosti systémov Linux a Unix (v závislosti od vybavenia zložky).
- Znalosti systémov Windows (v závislosti od vybavenia zložky).
- Znalosti vybavenia infraštruktúry siete.
- Znalosti internetových aplikácií (jednoduchý protokol transferu pošty – SMTP (Simple Mail Transfer Protocol), hypertextové prenosové protokoly – HTTP (HyperText Transfer Protocols),

V našich podmienkach okrem psychológa to bude špecializovaný technik, bezpečnostný expert (s praxou) a ekonóm, aby bolo nájdené správne riešenie konkrétnych prevádzkových problémov.

Vychádzame z komplexnej charakteristiky činnosti v priemysle komerčnej bezpečnosti a ich podmienok. Profesiografická metóda vychádza zo systematického pozorovania, sledovania kvantitatívnych a kvalitatívnych ukazovateľov, prevádzkových, výrobných a iných, využíva štatistiku a pod.. Rozbor profesie by mal prejsť aspoň týmito základnými etapami:

- celková charakteristika profesie,
- rozčlenenie profesie na základné a odborné činnosti, alebo ich časti,
- charakteristika základných profesionálnych činností, alebo ich časti,
- charakteristika psychických procesov a vlastností, ktoré sú závažné, prípadne i nežiaduce pre výkon profesie a k ním je možné dospieť na základe popisu a členenie profesie.

Z toho vyplýva, že by mal rozbor profesie obsahovať tieto časti:

- popis práce a súbor úloh a povinností,
- súpis znalostí a schopností, ktoré sú súčasťou prípravy na povolanie,
- zistenie pracovných podmienok,
- súhrn požadovaných telesných a duševných vlastností,
- vymenovanie vhodných osobných skúseností z predošlej praxe,
- vyjadrenie zodpovednosti pracovníkov profesie voči spoločnosti.

---

protokol pre prenos súborov – FTP (File Transfer Protocol), telnet (protokol pre vzdialený prístup), zabezpečený protokol pre terminálovú emuláciu – SSH (Secure Shell) atď.).

- Znalosti ohrozenia bezpečnosti (distribuovaný útok typu odoprenia služby – DDoS (Distributed Denial of Service), phishing (on-line krádež identity), poškodenie povrchovej úpravy (defacing), odpočúvanie sieťovej komunikácie (sniffing) atď..
- Znalosti hodnotenia rizík a praktických realizácií.

Ďalšie schopnosti

- Ochota pracovať 24 hodín denne, 7 dní v týždni na zavolanie (v závislosti od modelu služieb).
- Maximálna cestovná vzdialenosť (v prípade havárie pohotovosť v kancelárii; maximálna cestovná doba).
- Úroveň vzdelania
- Skúsenosti v práci v oblasti bezpečnosti IT. (5)

2.2.1 Všeobecná charakteristika práce

- Technická úroveň práce (remeselný, strojná, automatizovaná),
- intelektuálna úroveň práce,
- celková náročnosť:
  - zaťaženie psychické a fyzické
  - pracovná poloha,
  - pracovná doba a jej členenie,
  - pracovné tempo,
  - premenlivosť pracovných úloh,
  - pracovné ohrozenie,
  - bezpečnostné opatrenia,
- faktory vonkajšieho prostredia (pracovná poloha, osvetlenie, hluk, vibrácie a pod.),
- celkové spoločenské pracovné podmienky (formy spolupráce, hodnotenie),
- kvalifikačné nároky,
- predpísané preverenie pracovnej spôsobilosti.

2.2.2 Obsah pracovnej činnosti

- Vykonávanie špecializovaných a pomocných operácií a úkonov,
- plánovanie a riadenie činnosti,
- kontrola priebehu prác,
- kontrola chodu strojov a zariadení,
- kontrola výsledkov pracovnej činnosti.

2.2.3 Predmet práce

- Predmet práce spočíva v dopravovaní, zmene tvarov, montáži, riadení a ovplyvňovaní pracovníkov, výkonu služieb a rôznych iných činností.

2.2.4 Nároky

- Na psychické procesy a vlastnosti všeobecne od jednoduchej až po náročnejšiu prácu,
- na motoriku človeka z fyziologického a psychologického hľadiska,
- nároky na psychické procesy a vlastnosti.

2.2.5 Požiadavky na vlastnosti osobnosti

- Individuálna práca aj jej druh,
- kolektívna práca a jej druh.

2.2.6 Telesné požiadavky

- Telesná spôsobilosť,
- telesná zdatnosť,
- telesné schopnosti.

2.2.7 Duševné požiadavky

- Obecné nadanie,
- zvláštne duševné schopnosti,
- prístup. (2)

3 METÓDY BEZPEČNOSTNÉHO PRIESKUMU

Metódy bezpečnostného prieskumu sú systematickým, štruktúrovaným, formalizovaným a organizovaným prístupom ku zberu, analýze a následnej syntéze získaných informácií o skúmanej entite. Popisované metódy bezpečnostného prieskumu sú volené vzhľadom na praktickú využiteľnosť pre menšie organizácie, ktoré prieskum realizujú vzhľadom na ich možnosti z pohľadu know how, dostupnosti ľudských zdrojov, ekonomických možností a časového rámca pre realizáciu bezpečnostného prieskumu.

3.1 Bezpečnostná prehliadka (Safety Review: SR)

Bezpečnostná prehliadka je dôsledné, kritické posúdenie vybraných aspektov entity.

Účelom bezpečnostnej prehliadky je:

- vykonať hodnotenie zavedených procesov,
- vyhľadávať a identifikovať zmeny v zavedených procesoch,
- vyhľadávať a identifikovať nové zdroje rizík,
- vyhľadávať a identifikovať zmeny a v známych zdrojoch rizík.

Metódou zberu informácii je vizuálne skúmanie s využitím kontrolných zoznamov a pripravených matíc pre hodnotenie zavedených procesov a zaznamenanie zmien.

Výsledkom sú popisy možných problémov a podnety na ich nápravu. Bezpečnostní špecialisti by mal ovládať bezpečnostné štandardy a postupy organizácie, aby mohli zaznamenať odchýlky od schválených postupov a projektových zámerov.

3.2 Analýza kontrolným zoznamom (Checklist Analysis)

Táto metóda používa zoznam položiek alebo krokov, ktoré slúžia na overenie stavu systému. Je použiteľná v každom štádiu života systému. Kontrolné zoznamy by mali byť vytvárané viacerými autormi s rozličnou špecializáciou, ktorí by mali mať skúsenosti s danými systémom. Môžu byť vypracované pre celý systém, alebo len pre jednotlivé časti, pričom sa musí dbať na to, aby boli odhalené všetky zdroje možných problémov.

Účelom kontrolného zoznamu je predovšetkým porovnanie organizácie s praxou, ktorá je štandardná v podobných organizáciách. Ak chceme získať vyčerpávajúci zoznam rizík, je potrebné analýzu kontrolným zoznamom doplniť ďalšou metódou.

Pri vytváraní kontrolného zoznamu analytici definujú štandardné projektové alebo prevádzkové postupy a na základe tohto zoznamu formulujú otázky, ktorými sa snažia odhaliť nedostatky alebo rozdiely. Vyplnený kontrolný zoznam potom obsahuje odpovede na tieto otázky, ktoré môžu byť: „áno“, „nie“, „neaplikovateľný“ alebo „sú potrebné ďalšie informácie“. Skúsený manažér na základe týchto odpovedí určí ďalší postup. (5)

3.3 Brainstorming

Brainstorming je technikou tvorivého myslenia. Ide o metódu voľnej, spontánnej diskusie na danú tému. Je založená na hľadaní nových nápadov a návrhov a ich tvorivom kombinovaní a zlepšovaní. Pre použitie metódy brainstormingu je potrebné najprv definovať problém a vybrať osoby, ktoré budú problém riešiť.

Ďalšie prístupy:

a) Definícia problému sa nedešifruje do konkrétnych otázok, ale celý problém sa len konkrétne charakterizuje a určí sa, čo je potrebné vyriešiť prípadne aj smer očakávaného riešenia.
b) Účastníci riešenia nemajú byť len špecialisti daného oboru, ale aj ľudia rôznej kvalifikácie, ktorá ale má vzťah k riešenému problému.
c) Počet účastníkov nemá byť menší než 5 osôb, mal by byť v rozmedzí 5-12 až niekoľko desiatok osôb. Menší počet osôb zaručuje kolektívne posúdenie problému, na druhej strane zase nepresahuje možnosť aktívneho jednania a opakovania názorov. Dĺžka trvania by mala byť maximálne 3 hodiny a to v dobe, keď sa účastníci necítia byť viazaní plnením iných úloh.
d) Je potrebné odstrániť všetko, čo obmedzuje kreatívne myslenie členov. Je potrebné vylúčiť z procesu osoby zainteresované na niektorom spôsobe riešenia. Ďalej je potrebné vylúčiť osoby medzi ktorými je vysoký stupeň hierarchickej závislosti.
e) Z diskusie je nutné odstrániť kritikov názorov druhých účastníkov, polemík i zajímanie jednoznačných stanovísk.
f) Cieľom procesu je stanoviť pre daný problém čo najviac spôsobov riešenia.
g) Všetky názory sú zaznamenávané bez vzťahu k ich autorstvu nikto necíti byť viazaný tým čo v procese navrhol.

Vyhodnotenie všetkých zhromaždených materiálov, názorov nevykonávajú účastníci procesu, ale vybraní špecialisti, ktorí názory triedia, hodnotia možnosť realizácie podľa

určitých kritérií, rozhodnú o tom, ktoré názory je potrebné ďalej spracovávať, prípadne ich ihneď odporučia pre prijatie. (6)

3.4 Metóda Synectics

Hlavný princíp je podobný brainstormingu, to znamená, že je založená na uvoľnení kreatívneho myslenia. Líši sa spravidla procedúra postupu. Na rozdiel od brainstormingu tu nejde o vyvolanie akýchkoľvek asociácií, ale o intenzívne vybavovanie si analogických situácií v mysli zúčastnených riešiteľov. Ide teda o druh metódy poznania, ktorú je možné zahrnúť medzi metódy založené na analógii, na osobnej analógii členov skupiny, ktorí postupujú týmto spôsobom. Konštrukcia metódy vychádza z predpokladu, že ľudia dokážu myslieť iba v tých pojmoch, ktoré si dokážu predstaviť na základe určitej skúsenosti, ktorú dokážu vyjadriť. Počas procesu kreatívneho riešenia tohto problému kombinujú tieto známe pojmy, prenášajú ich z jedných situácii do druhých. Pri použití tejto metódy sa doporučuje voľba vhodného prostredia, t.j. uvoľnená atmosféra, ale už menší kolektív riešiteľov v rozmedzí 2 až 6 osôb, z ktorých jedna je poverená riadiacou funkciou. Riešitelia nemusia byť špecialistami v technickom riešení problému, pretože formuláciu dostávajú rozpracovanú z miesta, kde problém vznikol. Ich úlohou nie je prepracovať určité riešenie až k praktickej aplikácii, ale nájsť hlavný spôsob tohto riešenia.

Elementárne fáze postupu sú:

a) Špecialisti sformulujú vzniknutý problém v pojmoch, ktoré sú zrozumiteľné účastníkom riešiteľského tímu.
b) Tím problém zanalyzuje a zisťuje, čo má riešenie problému priniesť.
c) V ďalšej fáze sa tím snaží vyfiltrovať svoje myslenie od spontánnych nápadov pokiaľ prídu k názoru, že tieto smery riešenia sú bezvýchodiskové. Toto je dôvod prečo je volená metóda Synectics, ako cesta hľadania iného riešenia.
d) Tím potom sformuluje jadro problému do elementárnej názorovej podoby, na ktorej sa zhodne.
e) Na základe predchádzajúcej formulácie tím hľadá prvú priamu analógiu riešenia podobného prípadu v zásobe svojich skúseností, a to tak, že pri riešení technického, alebo bezpečnostného problému hľadajú najprv analógiu v prírode, alebo v praxi a naopak v prípade riešenia ekonomického problému postupujú tak, že hľadajú priame analógie v mikroštruktúre u makroproblémov a naopak.

f) Všetci účastníci tímu sa v ďalšej fáze vmyslia do všetkých nájdených analógií (osobných analógií všetkých členov tímu) a snažia sa ich symbolicky stručne vyjadriť a to v odstupe od zadaného problému tak, aby vzniklo jadro analogického prípadu. V niektorých prípadoch vedie prvá priama analógia k nájdeniu nových hľadísk riešenia problému a to po vykonaní analýzy analógiou a jej vzťahov k riešeniu problému.
g) Pokiaľ prvá priama analógia nepriniesla uspokojivé výsledky, vykoná sa v ďalšej fáze druhá priama analógia, ktorá zmení spôsob čerpania pojmov zo zásoby tímu t.j. technickú analógiu vystrieda analógia prírodná.
h) Novo objavené analógie sa opäť analyzujú a konfrontujú s vlastnou formuláciou problému s cieľom nájsť nové hľadiská pre riešenie tohto problému. (6)

3.5 Brainwriting

Je založená na princípe kolektívneho vybavovania myšlienok. Metóda spočíva v písomnom prejave viacerých osôb, zameranom na riešení tej istej úlohy. Postup tejto metódy vychádza zo sformulovanej úlohy, ktorej riešenie hľadá 6 osôb zvolených tak, aby sa líšili skúsenosťami, vzdelaním, profesiou, vekom, prípadne inými vlastnosťami, ktoré majú vplyv na spôsob riešenia úlohy.

Jednotlivé kroky postupu sú:

a) Hlavné problémy úlohy sú rozpísané do formulára tak, aby bolo uľahčené rýchle spísanie náčrtu ich riešenia.
b) Formulár je rozdaný šiestim osobám, ktoré sú zvolené podľa už zmieneného kľúča, osoby sú sústredené v tej istej miestnosti.
c) Každý účastník vpíše do svojho formulára návrh troch možných spôsobov riešenia problém a to v predpísanom časovom limite 3-5 minút.
d) Účastníci sediaci okolo stola si vzájomne vymenia formuláre v smere hodinových ručičiek. Predpokladá sa, že účastníci na riešení problému
    a. Rozvinú riešenie predošlého účastníka.
    b. Uvedú dôvody, prečo nie je možné riešenie predošlého účastníka uskutočniť.
    c. Pridajú náčrt nového riešenia.

Čas vymedzený na splnenie týchto úloh je 3-5 minút.

e) Posun formulárov môže pokračovať spôsobom uvedeným v bode d). (6)

3.6 Metóda Delphi

Metóda Delphi je štruktúrovaná komunikačná technika expertov vyvinutá pre systematické predpovede pravdepodobností udalostí. Je to prognostická metóda. Určuje čo sa môže stať a za akých podmienok, využíva sa pre generovanie nových myšlienok. Spočíva v riadenom kontakte medzi expertmi hodnotiaceho tímu a hodnoteného subjektu.

Podstata:

- Expert pracuje individuálne a anonymne, odpovedá na písomnú anketu.
- Expertíza má niekoľko etáp, po každej etape sa výsledky spracujú a s názormi všetkých expertov sa jednotlivci zoznamujú. Potom každý jednotlivec si premyslí svoj názor z hľadiska prvej etapy, ktorý musí prísne vyargumentovať, alebo ho odmietnuť a prijať kompromis. O výsledku prvej etapy sa spracuje zápis a každý sa v ňom zoznamuje s výsledkami celej skupiny. Každý má zase premyslieť svoj záver. Za optimálne sa považujú 3-4 etapy tejto činnosti. Ak sa názory expertov nezbližujú ani po 4 etapách, expertná činnosť sa ukončuje a záver je ten, že skupina nebola zložená správne. Obvykle ale vo štvrtej etape sa výrazná väčšina názorov zhoduje.

Hodnotenie výsledkov expertízy:

V danej situácii nie je možné slepo veriť väčšine, ani názorom jednotlivcov. Obvykle sa za objektívnu považuje skupina 4-20 expertov. Táto činnosť sa využíva v práci špecializovaných expertov podnikov priemyslu komerčnej bezpečnosti zaoberajúcich sa analytickou, expertnou, audítorskou, alebo konzultačnou činnosťou. Získané výsledky expertízy majú prognostický, pravdepodobnostný charakter. (1)

3.7 Relatívne hodnotenie (Relative Ranking – RR)

Relatívne hodnotenie je skôr analytická stratégia, než analytická metóda. Jej účelom je z hľadiska bezpečnosti stanoviť relatívnu dôležitosť procesov a činností a na jej základe posúdiť potrebu ďalších analýz. Medzi metódy relatívneho hodnotenia nebezpečenstva patria napr. metódy využívajúce Do Fare and Explosion Index, (Dowov index horľavosti a výbušnosti), Mond Index (Mondov index), Substance Hazard Index (Index nebezpečnosti látky), Chemical Explosure Index (Index pôsobenia chemických vplyvov) apod. Na

základe použitej metódy je výsledkom analýzy zoznam procesov, zariadení a činností zoradených podľa úrovne dôležitosti, stupnice faktorov, grafy a pod.. (5)

3.8 Predbežná analýza zdrojov rizika (Preliminary Hazard Analysis - PHA)

Používa sa v prípade, že je dispozícii málo dostupných údajov o procese, teda vo fáze jeho vývoja a slúži ako podklad pre ďalšie analýzy. Účelom PHA je zostaviť zoznam zdrojov rizika, pričom nebezpečné situácie v tomto zozname budú zoradené v závislosti od miery rizika. Ak chce organizácia znížiť alebo obmedziť nebezpečenstvo, musí zamerať najväčšiu pozornosť situáciám na začiatku zoznamu. Pre vykonanie analýzy potrebujú analytici informácie o položkách vstupujúcich do procesu (suroviny, medziprodukty), o výstupných položkách (konečné produkty), prevádzkových podmienkach, zaradeniach a prostredí, ako aj o projektových kritériách procesu. (5)

3.9 Analýza „Čo sa stane, keď“ (What If – WI)

Táto metóda je založená na spontánnej diskusii skupiny ľudí, ktorí sú dobre oboznámení

s procesom. Môže byť použitá v každom štádiu života procesu pričom analytici sa pomocou kladenia otázky „Čo sa stane keď“ snažia odhaliť možné nežiaduce udalosti, ktoré by mohli predstavovať zdroj rizika. Aby otázky čo najvyčerpávajúcejšie analyzovali systém, je potrebné, aby analytici mali k dispozícii nákresy a popisy procesu. Otázky a odpovede sa následne rozdelia podľa následkov do viacerých oblastí, napr. bezpečnosť zamestnancov, požiarna ochrana, ... a navrhnú sa spôsoby zníženia rizika. Zoznam otázok a odpovedí môže mať tiež tabuľkovú formu, kedy nebezpečné situácie nie sú zoradené podľa dôsledkov nehodových scenárov. Takýto zoznam poukazuje na možnosti ochrany proti následkom nebezpečných udalostí a obsahuje návrhy pre zníženie rizika. (5)

3.10 Štúdia nebezpečenstva a prevádzkyschopnosti (Hazard and Operability Analysis -HAZOP)

Štúdia HAZOP bola vyvinutá pre chemický priemysel. Využíva sa na určenie potenciálneho nebezpečenstva a problémov obmedzujúcich prevádzkyschopnosť spôsobených odchýlkou od navrhnutého účelu, tak pre nové ako aj existujúce prevádzky.

Projektové a prípravné práce predchádzajúce uvedeniu určitého procesu do prevádzky sú

často vykonávané pod veľkým časovým tlakom. Tento tlak môže spôsobiť nedbalosť a chyby. Štúdia HAZOP poskytuje možnosť zistiť a opraviť tieto chyby ešte predtým, ako by spôsobili vysoké škody na majetku, zdraví alebo životnom prostredí.

Výhody HAZOPu spočívajú v:

- jednoduchosti – metódu si pracovník zúčastňujúci sa štúdie dokáže jednoducho osvojiť,
- širokej použiteľnosti – metóda môže byť využitá pri analýze takmer všetkých činností,
- ktoré sa uskutočňujú v rámci pracovného procesu.

Metóda spočíva v popise procesu a systematickom kladení otázok týkajúcich sa každej časti procesu. Na ich základe sa určia odchýlky od navrhnutého účelu a negatívne následky týchto odchýlok ovplyvňujúce bezpečnosť a prevádzkyschopnosť zariadení.

Pri kladení otázok sa používajú kľúčové slová, ktoré môžeme rozdeliť na:

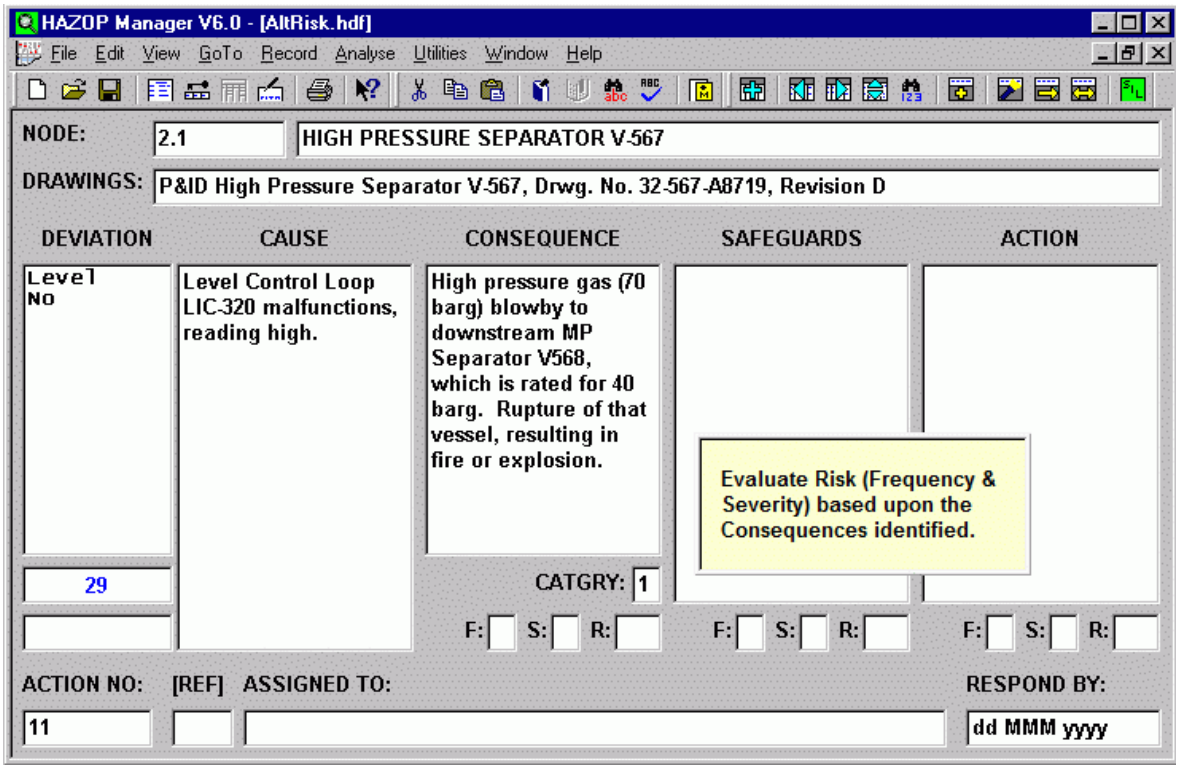
- primárne, ktoré zameriavajú pozornosť na čiastkové hľadiská navrhnutého účelu alebo na celkové parametre a podmienky procesu,
- sekundárne, ktoré, ak sa skombinujú s primárnymi, upozornia na možné odchýlky.

Zoznam štandardných kľúčových slov:

No (žiadny): Navrhnutý účel nebol realizovaný (napr. Flow/No – žiadny prietok), alebo funkčné hľadisko nie je dosiahnuteľné.

- Less (menej, menší): Vyskytol sa kvantitatívny úbytok oproti navrhnutému účelu (napr. Pressure/Less – nižší tlak).
- More (viac, vyšší): Vyskytol sa kvantitatívny nárast oproti navrhnutému účelu (napr. Temperature/More – vyššia teplota)
- Reverse: (opačný, spätný): Nastal opak navrhnutého účelu (napr. Reverse/Flow – spätný prietok).
- Also: (tiež, okrem) Navrhnutý účel je kompletne splnený, ale prejavila sa ďalšia súvisiaca činnosť (napr. Flow/Also – kontaminácia produktu.
- Other: (iný): Realizovala sa úplne iná činnosť, ako sa očakávalo (napr. Flow/Other priesak materiálu, Composition/Other – nevhodné rozmery suroviny)
- Fluctuation: (výkyv, kolísanie): Požadovaný účel sa dosahuje len čiastočne.

- Early: (skorý): Zvyčajne sa používa pri analýze nepretržitých činností a určuje situáciu, ktorá začala v zlom čase alebo nenadväzovala.
- Later: (neskorý): Zvyčajne sa používa pri analýze nepretržitých činností a určuje situáciu, ktorá začala v zlom čase alebo nenadväzovala.



Obrázok 3: softvérový nástroj Hazop Manager

Výsledky sa zaznamenávajú do tabuľky zo štruktúrou stĺpcov: Deviation: odchýlka, Cause: príčina, Consequence: následok, Safeguards: ochrana, Action: činnosť. (5)

3.11 Analýza porúch a ich dôsledkov (Failure Mode and Effect Analysis – FMEA)

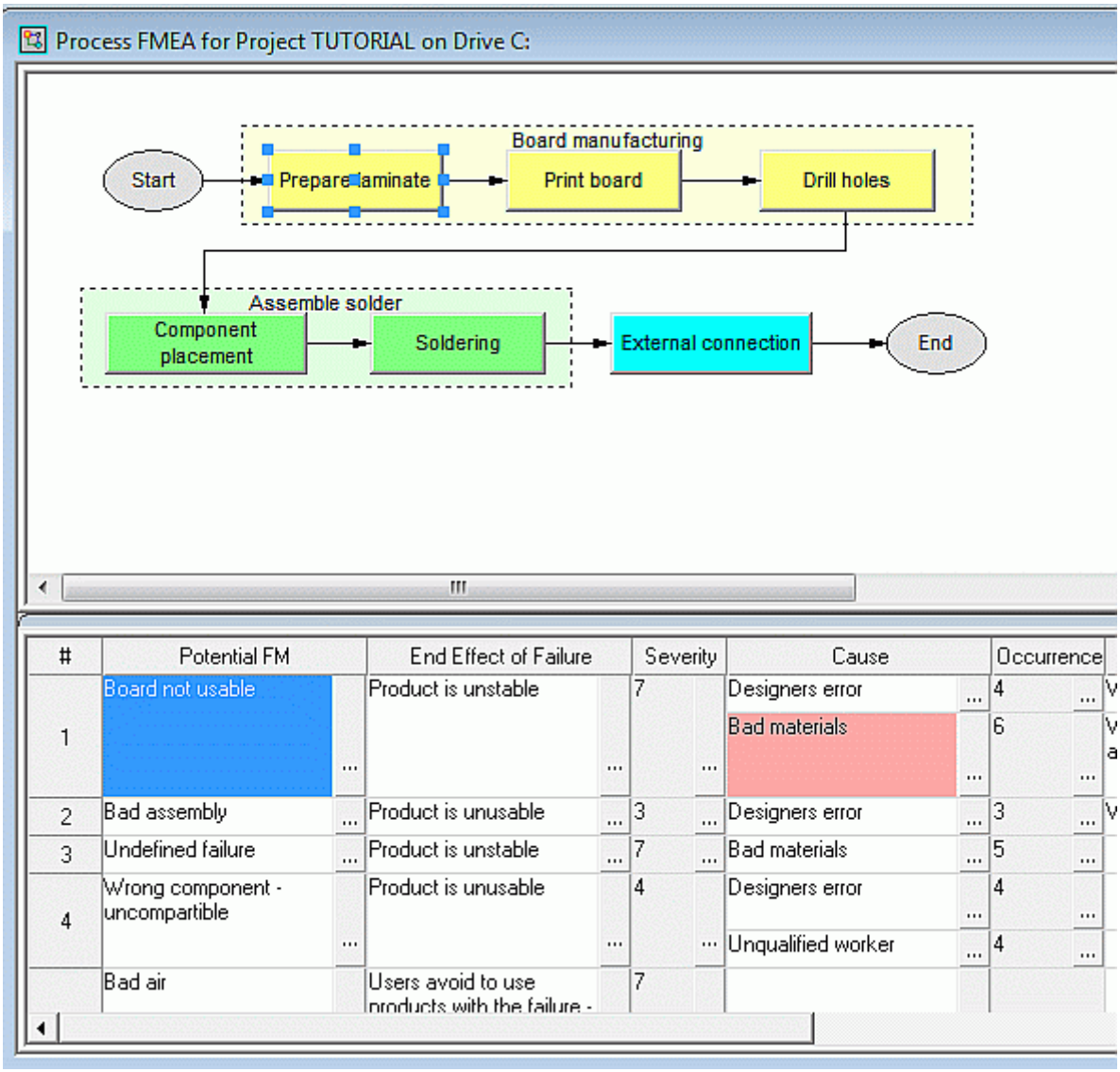
Na základe tejto metódy je možné systematicky identifikovať možné poruchy systému alebo procesu. Používa sa vo výrobných podnikoch počas rôznych životných fáz procesu, napríklad v automobilovom priemysle. Pri navrhovaní systému je úlohou FMEA zabrániť budúcim škodám. Neskôr sa využíva v procese kontroly.

POTENTIAL FAILURE MODE AND EFFECTS ANALYSIS — **PROCESS FMEA**

FMEA Number:		Responsibility:	ALD	FMEA Date:	01.10.2001
Item:	Start	Prepared by:	Alex	Key Date:	01.01.2002
Project:	TUTORIAL	Core team:	ALD software development department	Last review:	01.11.2001

Item name	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Potential Causes of Failure	OCC	Current Controls	DET	RPN	Recommended Actions: Description	Recommended Actions: Reponsible & Target Date	Actions Taken	SEV	OCC	DET	Res. RPN
Start	Can not start	Nothing is done	10	Bad materials	5	Visual inspection	6	300	>Increase quality requirements for materials		Increase quality requirements for materials	10	4	3	120
				Designers error	3	Visual inspection	6	180	>Technical inspection before documentation release	Technical engineer	Technical inspection before documentation release	10	7	2	140
									Every 2 weeks, refresh inventory	Materials					
									Place boards in protective packaging						
	Short circuit	Product is unstable	7												

Obrázok 4: výstupná zostava FMEA, softvér Ram commander



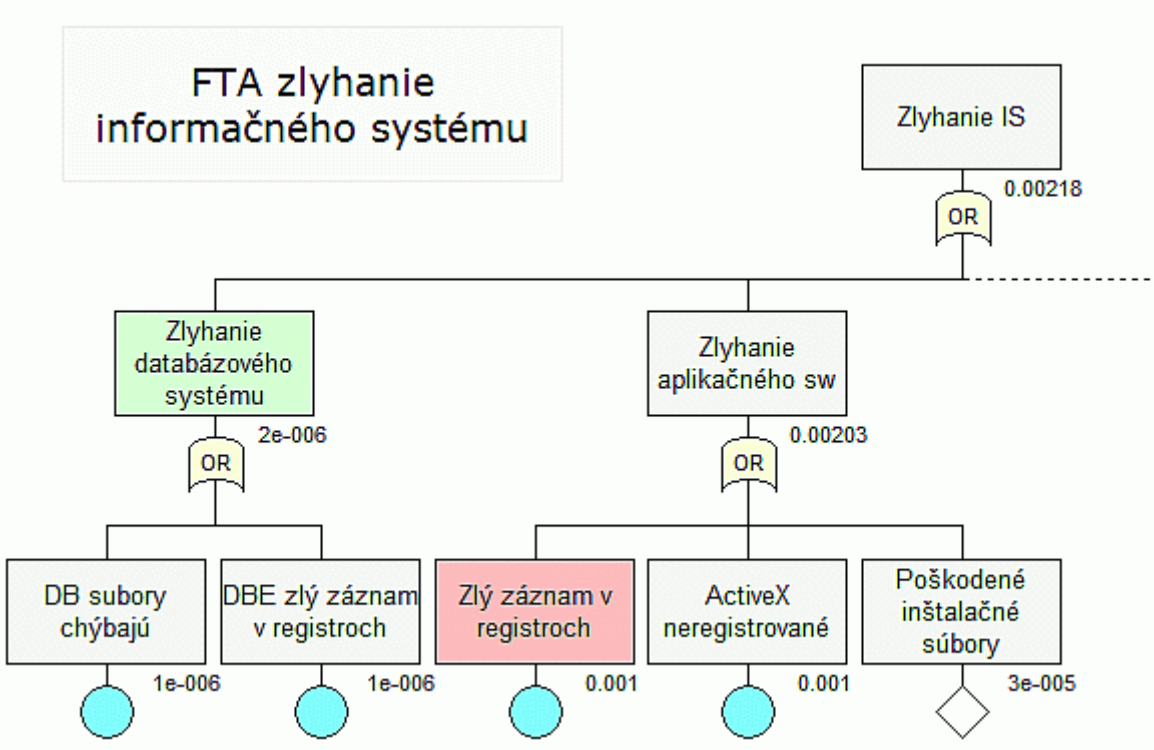
Obrázok 5: FMEA softvér Ram commander, tvorba procesu

Poruchový stav (Failure Mode) nastáva vtedy, keď zlyhá systém ako celok alebo niektorý z jeho komponentov. Za poruchy považujeme skutočné alebo potenciálne chyby a poškodenia, no predovšetkým tie, ktoré môžu postihnúť zákazníka.

Analýza dôsledkov sa vzťahuje na určenie dôsledkov týchto porúch. Účelom analýzy je identifikovať poruchy zariadení alebo systému a ich možné dôsledky vplývajúce na systém alebo podnik. Poruchy sa zoradia v závislosti od významnosti ich dôsledkov, frekvencie výskytu a náročnosti ich odhalenia. Následne sa vytvoria odporúčania pre zvýšenie spoľahlivosti zariadení a tým aj pre zlepšenie bezpečnosti procesu. Aby bolo možné analýzu vykonať, je potrebné aby analytici boli oboznámení s funkciami zariadenia a s tým, ako môže zariadenie ovplyvniť systém. Výsledkom analýzy je zoznam porúch a ich následkov, ktorý sa zvyčajne zapisuje do tabuľky. (5)

3.12 Analýza stromu porúch (Fault Tree Analysis – FTA)

FTA je grafický model, ktorý zobrazuje rôzne kombinácie chýb zariadení a ľudských chýb, ktoré môžu vyústiť do systémovej poruchy, ktorú označujeme ako vrcholová udalosť. Analýza je vhodná pre veľké systémy. Výsledkom analýzy je zoznam kombinácií chýb, ktoré nazývame aj kritické rezy.



Obrázok 6: softvér Ram commander FTA zlyhanie softvéru

Tento zoznam získa analytik z modelov stromov porúch, ktorých počet je závislý od zložitosti posudzovaného zariadenia alebo systému. Na základe posúdenia zoznamu kritických rezov môže analytik navrhnúť opatrenia na zníženie rizika.

K tomu potrebujú podrobné nákresy procesov a postupov a znalosť možností zlyhania jednotlivých častí zariadení a dôsledky týchto zlyhaní. Ak analýzu vykonáva len jeden človek, je nevyhnutné, aby výsledné modely posúdili pracovníci, ktorí majú skúsenosť s prevádzkou rovnakých alebo podobných zariadení a procesov, ako boli analyzované. (5)

3.13 Analýza stromu udalostí (Event Tree Analysis - ETA)

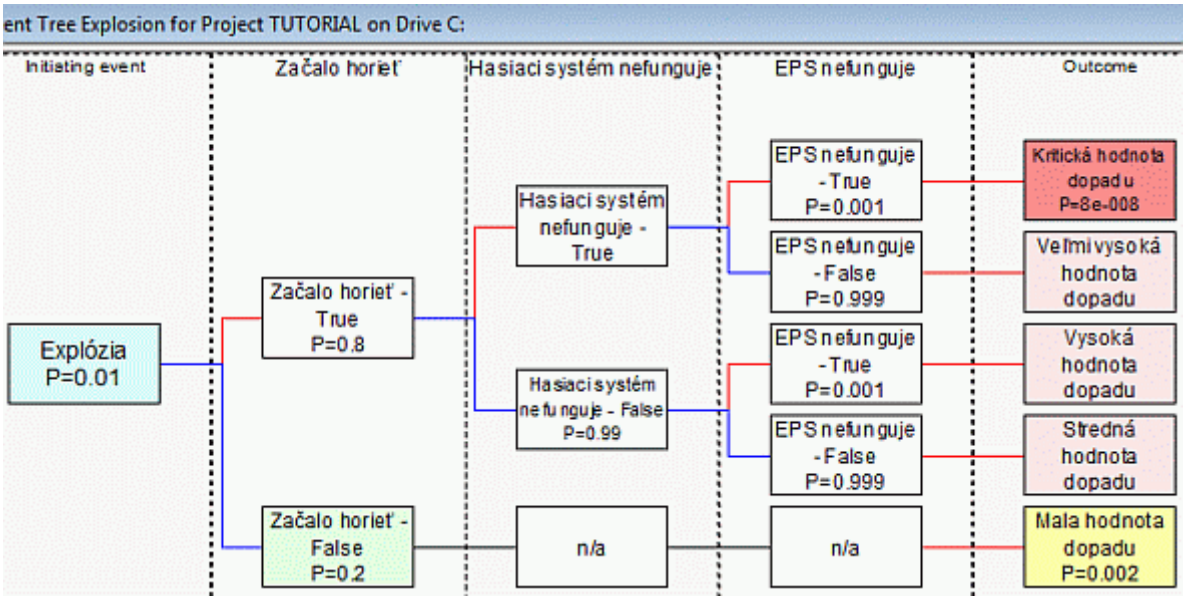
Strom udalostí je grafický logický model, ktorý identifikuje a kvantifikuje možné výsledky iniciačnej udalosti prostredníctvom konštrukcie udalostí vždy na základe dvoch možností: priaznivo, alebo nepriaznivo.

Zobrazenie stromu udalostí predstavuje rozvetvený graf s určenou symbolikou a popisom.

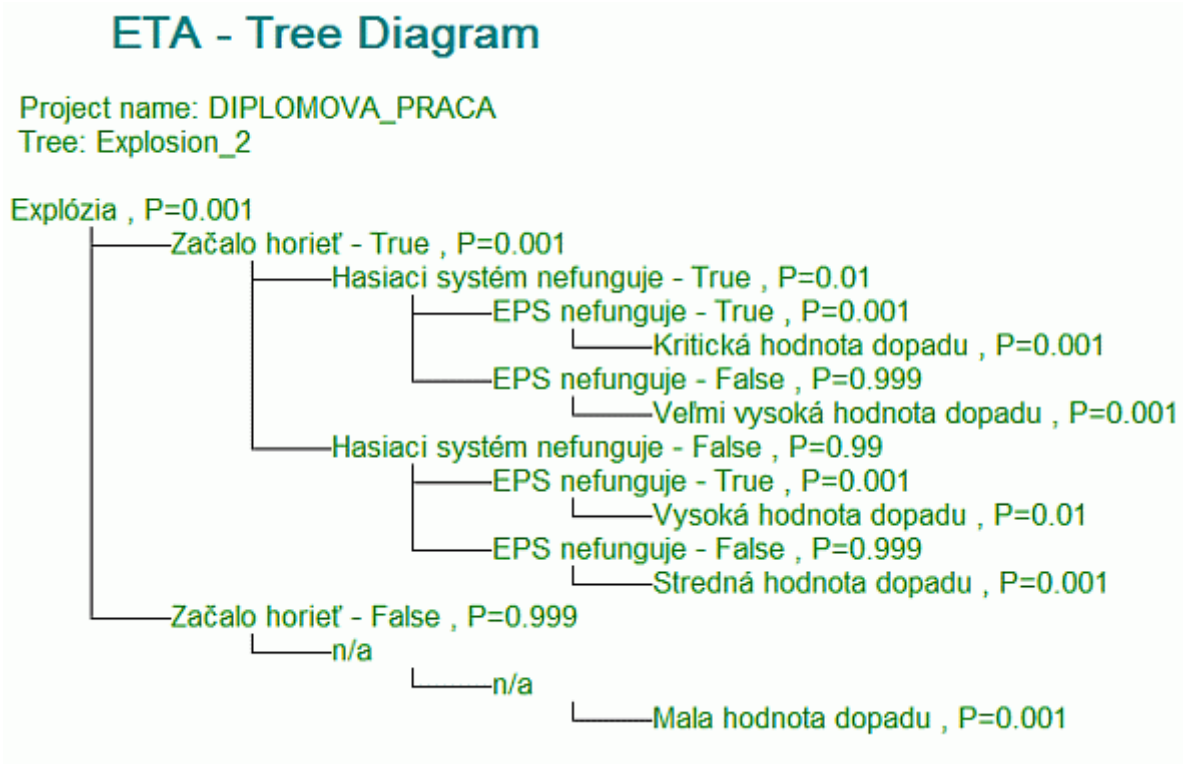
Znázorňuje všetky udalosti, ktoré sa môžu v posudzovanom systéme vyskytnúť. Je vhodná pre systémy, ktoré majú zavedené bezpečnostné systémy, alebo havarijné plány pre zásah v prípade reakcie na počiatočné udalosti mimoriadnej udalosti, alebo pre modelovanie časovej závislosti medzi zlyhaniami a udalosťami v postupnosti mimoriadnej udalosti.

Postup:

- Identifikácia a definícia závažných náhodných udalostí, alebo jav, ktoré môžu viesť k dôsledkom. Tieto náhodné udalosti môžu byť identifikované a ohodnotené niektorou z metód analýzy rizík.
- Definovať javy, ktoré môžu spôsobiť náhodné udalosti.
- Vytvoriť strom udalostí.
- Analyzovať strom porúch: preskúmanie štruktúry stromu porúch.
- Dokumentácia výsledkov: popis analyzovaného systému, potenciálnych výsledkov nepredvídanej udalosti, určenie frekvencie náhodnej udalosti a pravdepodobnosť vetvy v strome udalosti, výpočet pravdepodobností pre identifikované následky, zhrnúť a prezentovať závery analýzy.



Obrázok 7: softvérový nástroj RAM Commander ETA

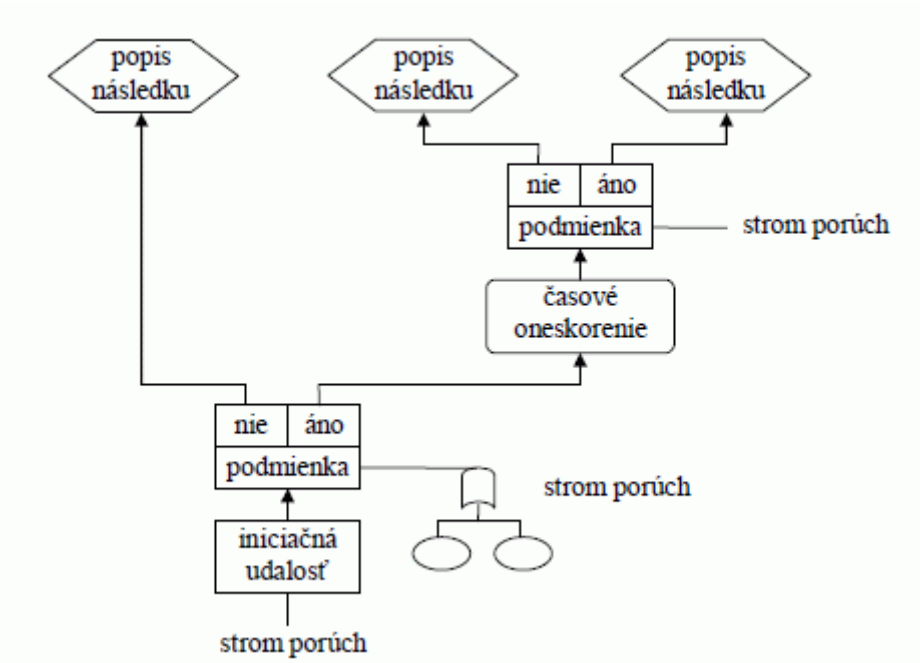


Obrázok 8: softvérový nástroj RAM Commander ETA, výstupná zostava

3.14 Analýza príčin a následkov (Cause Consequence Analysis – CCA)

Táto metóda kombinuje analýzu príčin (popísanú ako strom porúch) a analýzu dôsledkov (popísanú ako strom udalostí). Účelom metódy je odhaliť základné príčiny a následky

možných nehôd. Využíva pri tom diagramy príčin a následkov, ktoré zobrazujú vzťahy medzi koncovými stavmi nehody (následkami) a ich základnými príčinami.



Obrázok 9: Cause Consequence Analysis – CCA (5)

Táto metóda sa vzhľadom na jej detailnosť najčastejšie používa pri analýze jednoduchších systémov. Môže ju vykonávať jeden analytik, ale najčastejšie ju vykonáva skupina dvoch a štyroch ľudí. Jeden člen skupiny ovláda postup metódy CCA alebo ETA a ostatní členovia poznajú analyzovaný systém alebo zariadenie. (5)

3.15 Analýza spoľahlivosti človeka (Human Reliability Analysis – HRA)

Účelom analýzy spoľahlivosti človeka je identifikovať možné ľudské chyby a ich pôsobenie ako aj príčiny týchto chýb. Ide teda o systematické hodnotenie faktorov ovplyvňujúcich činnosť personálu pôsobiaceho vo výrobe (napr. operátorov, údržbárov, technikov). Výsledkom je zoznam chýb, ktoré sa môžu vyskytnúť počas bežnej alebo núdzovej prevádzky, faktorov prispievajúcich k týmto chybám a návrh zmien v systéme, ktoré prispejú k zníženiu pravdepodobnosti takýchto chýb. Analýzou sa teda identifikujú dôležité miesta systému, ktoré sú ovplyvnené chybami a následne sa určí poradie týchto chýb vo vzťahu k ostatným a to na základe pravdepodobnosti výskytu alebo závažnosti ich následkov. Keďže pri výrobe človek pôsobí svojim konaním na zariadenia, často sa HRA kombinuje s metódami, ktoré odhaľujú zdroje rizika zariadení a procesov, napr. s metódami ETA, FTA, HAZOP alebo FMEA. (5)

II. PRAKTICKÁ ČASŤ

4 MODEL, SIMULÁCIA BEZPEČNOSTNÉHO PRIESKUMU FIKTÍVNEJ ORGANIZÁCIE PRE SPRACOVANIE BEZPEČNOSTNÉHO PROJEKTU INFORMAČNEJ BEZPEČNOSTI

4.1 Cieľ bezpečnostného prieskumu

Cieľom bezpečnostného prieskumu je získanie informácií pre vypracovanie bezpečnostného projektu informačnej bezpečnosti podľa STN ISO/IEC 27001 a to:

- Identifikovať a hodnotiť aktíva, ktoré majú byť chránené,
- Identifikovať a hodnotiť hrozby, ktoré môžu na aktíva pôsobiť.
- Identifikovať a hodnotiť úroveň implementácie prijatých bezpečnostných opatrení.
- Identifikovať a hodnotiť riziká pôsobiace na aktíva.

Bezpečnostný projekt informačnej bezpečnosti je plán pre zavedenie systému riadenia informačnej bezpečnosti v organizácii. Cieľom spracovania bezpečnostného projektu informačnej bezpečnosti je:

- Posúdiť súčasný stav bezpečnosti informácií organizácie.
- Definovať minimálnu požadovanú úroveň bezpečnosti informácií organizácie.
- Navrhnúť opatrenia podľa priorít pre dosiahnutie minimálnej požadovanej úrovne bezpečnosti informácií.
- Navrhnúť opatrenia pre udržanie a zvyšovanie úrovne bezpečnosti informácií.

Požiadavkou je, aby bezpečnostný projekt informačnej bezpečnosti bol spracovaný v súlade z:

- Zákonom č. 275/2006 Z.z. o informačných systémoch verejnej správy.
- Výnosom Ministerstva financií Slovenskej republiky z 9. júna 2010 č. 312/2010 o štandardoch pre informačné systémy verejnej správy, časť: Bezpečnostné štandardy, štandardy pre architektúru riadenia.
- Zo Zákonom č.428/2002 Z.z., č.90/2005 Z.z o ochrane osobných údajov a berie na zreteľ oznámenie Ministerstva zahraničia č.49/2001 o prístupe k Dohovoru Rady Európy č. 108 o ochrane jednotlivca pri automatizovanom spracovaní osobných údajov.

- STN ISO/IEC 27001 Informačné technológie, zabezpečovacie techniky. Systémy manažérstva informačnej bezpečnosti.
- STN ISO/IEC 27002 Informačné technológie, zabezpečovacie techniky. Pravidlá dobrej praxe manažérstva informačnej bezpečnosti. (bývalá ISO/IEC 17799:2005)
- STN ISO/IEC TR 13335-3 Informačné technológie, návod na manažérstvo bezpečnosti IT. Časť 3: Techniky pre manažment bezpečnosti IT

4.2 Predbežný prieskum

Účelom predbežného prieskumu je získať informácie pre určenie stratégie, metód a plánovanie bezpečnostného prieskumu.

- Identifikovať predstavy manažmentu o očakávaniach z výsledku bezpečnostného prieskumu.
- Identifikovať problémové oblasti organizácie z pohľadu informačnej bezpečnosti.
- Identifikovať schopnosť kooperácie partnera.
- Získať záväzok manažmentu o podpore činností bezpečnostného prieskumu.
- Získať základné informácie o spoločnosti jej organizačnej štruktúre.
- Získať informácie o roliach vedúcich pracovníkov v jednotlivých oblastiach o rozsahu ich zodpovedností.
- Získať menný zoznam vedúcich pracovníkov a kontaktné údaje na nich.
- Získať kópie dokumentov bezpečnostných politík, bezpečnostných smerníc jednotlivých oblastí pre prípravnú fázu bezpečnostného prieskumu.

4.3 Prípravná fáza bezpečnostného prieskumu

4.3.1 Presné vytýčenie cieľa bezpečnostného prieskumu

Cieľom bezpečnostného prieskumu je v organizácii identifikovať a ohodnotiť aktíva, hrozby, riziká, úroveň prijatých bezpečnostných opatrení, preskúmať bezpečnostné oblasti definované podľa štandardu STN ISO/IEC 27002 a to:

- bezpečnostné politiky,
- organizáciu informačnej bezpečnosti,
- riadenie aktív,
- bezpečnosť ľudských zdrojov,
- fyzickú bezpečnosť a bezpečnosť prostredia,

- riadenie komunikácie a prevádzky,
- riadenie prístupu,
- vývoj a údržbu informačných systémov,
- riadenie incidentov informačnej bezpečnosti,
- riadenie kontinuity činnosti,
- súlad s technickými normami a právnymi predpismi.

4.3.2 Určenie stratégie, výber metodiky, projekt manažment bezpečnostného prieskumu

4.3.2.1 Výber metodiky bezpečnostného prieskumu

Pre získanie informácií z bezpečnostného prieskumu boli vybrané metódy:

Bezpečnostná prehliadka (Safety Review: SR)

Bezpečnostná prehliadka je dôsledné, kritické posúdenie vybraných aspektov entity.

Účelom bezpečnostnej prehliadky je:

- vykonať hodnotenie zavedených procesov,
- vyhľadávať a identifikovať zmeny v zavedených procesoch,
- vyhľadávať a identifikovať nové zdroje rizík,
- vyhľadávať a identifikovať zmeny a v známych zdrojoch rizík.

Metódou zberu informácii je vizuálne skúmanie s využitím kontrolných zoznamov a pripravených matíc pre hodnotenie zavedených procesov a zaznamenanie zmien.

Analýza kontrolným zoznamom (Checklist Analysis)

Táto metóda používa zoznam položiek alebo krokov, ktoré slúžia na overenie stavu systému. Je použiteľná v každom štádiu života systému.

Účelom kontrolného zoznamu je predovšetkým porovnanie organizácie s praxou, ktorá je štandardná v podobných organizáciách.

Informačný systém je popisovaný z hľadísk:

- aktív informačného systému – podľa vrstiev rozdelenia modelu OSI (STN ISO/IEC 7498),
- aktív informačného systému: písomná forma, elektronická forma (dáta),

- osôb - zamestnanci, dodávatelia, externisti,
- fyzického prostredia, fyzickej bezpečnosť budovy, jednotlivých miestností,
- činností, procesov.

Aktíva sú popisované z hľadísk:

- **Informácie:** všetky typy informácií spracovávaných v informačnom systéme.
- **Softvér:** operačné systémy, aplikácie pre spracovávanie informácií.
- **Hardvér:** kabeláž, sieťové prvky, hardvér serverov a pracovných staníc, podporné zariadenia.
- **Osôb:** používatelia (zamestnanci), používatelia tretích strán.
- **Písomná forma:** dokumentácia, informácie v písomnej forme.
- **Fyzického prostredia:** fyzická bezpečnosť popis perimetra fyzickej bezpečnosti, budovy, jednotlivých miestností.
- **Činností, procesov:** procesy informačnej bezpečnosti, procesy fyzickej bezpečnosti.
- **Poskytovaných služieb**: služby informačného systému.

4.3.2.2 Plánovanie, výber ľudí, projekt manažment

Na základe bezpečnostného predbežného prieskumu existuje predpoklad, že na realizáciu samotnej práce v teréne budú postačovať 3 návštevy bezpečnostných konzultantov. Chýbajúce informácie budú doplňované elektronickou formou komunikácie zo zástupcami príslušných organizačných celkov organizácie.

Vzhľadom na definované ciele bezpečnostného prieskumu t.j. získať informácie pre vypracovanie bezpečnostného projektu informačnej bezpečnosti podľa štandardu STN ISO/IEC 27001, budú na prieskume pracovať špecialisti:

- Projekt manažér, bezpečnostný špecialista primárne úlohy: riadenie procesu bezpečnostného prieskumu, analýza, spracovanie celkovej správy z prieskumu, komunikácia zo skúmanou organizáciou. Primárne preskúma bezpečnostné oblasti: organizácie informačnej bezpečnosti a riadenia aktív.
- Špecialista bezpečnosti informačných technológií primárne úlohy: preskúma bezpečnostné oblasti: riadenie komunikácie a prevádzky, riadenie prístupu, vývoj a údržba informačných systémov.

- Špecialista na bezpečnostné technológie primárne úlohy: preskúma bezpečnostné oblasti: fyzická bezpečnosť a bezpečnosť prostredia, riadenie incidentov informačnej bezpečnosti, riadenie kontinuity činnosti,
- Špecialista na posúdenie súladu z technickými normami a právnymi predpismi. Primárne preskúma bezpečnostné oblasti: súlad s technickými normami a právnym prostredím, bezpečnosť ľudských zdrojov, bezpečnostné politiky.

4.3.2.3 Ohlásenie návštevy

Dokument ohlásenia návštevy o bezpečnostnom prieskume poskytuje skúmanej organizácii informáciu o plánovanom priebehu bezpečnostného prieskumu. Poskytuje zoznam požadovaných dokumentov zo strany skúmanej organizácie. Ďalej poskytuje informáciu o potrebnom organizačnom zabezpečení zo strany skúmanej organizácie, poskytuje mená členov tímu, ktorí budú na bezpečnostnom prieskume pracovať, spôsob ich identifikácie na mieste bezpečnostného prieskumu. Tento dokument je v písomnej forme zaslaný manažmentu skúmanej organizácie. Manažment dokument vyplní a zašle podpísaný späť.

Tabuľka: obsah dokumentu ohlásenia návštevy.

Základné informácie o bezpečnostnom prieskume	
Cieľ bezpečnostného prieskumu	
Dátum, čas, miesto	
Hrubý časový rozvrh	
Skúmané bezpečnostné oblasti	
Vybrané metódy zberu informácii	
Požadované dokumenty	
Týka sa organizačných jednotiek	
Požadovaná prítomnosť osôb	
Mená členov tímu	
Sprievodca zo strany organizácie	

Tabuľka 1: obsah dokumentu ohlásenia návštevy.

Predbežné informácie k bezpečnostnému prieskumu	
Bezpečnostný projekt strážnej služby, prípadne smernice výkonu strážnej služby	
Smernice výkonu kľúčovej služby	
Smernice kontroly vstupu	
Požiarne smernice	
Prevádzkový poriadok objektu	
Revízie elektrických zariadení	
Mená vedúcich na pracoviskách	
Mená kontaktných osôb a pracovná doba	
Všeobecnú BP politiku organizácie	
BP politiku informačnej bezpečnosti	
BP jednotlivých IT systémov	

Tabuľka 2: požadované dokumenty a informácie k bezpečnostnému prieskumu

4.3.2.4 Príprava pre prácu v teréne

Príprava dokumentácie a nástrojov bezpečnostného prieskumu

Manažment organizácie, ktorá má byť preskúmavaná akceptoval oznámenie o návšteve, ktorej cieľom je bezpečnostný prieskum. Boli pripravené formuláre a dotazníky pre zvolené metodiky bezpečnostného prieskumu.

Budova popis IS	Spoločnosť:	Spracoval:
	X	**Daniel Bednárik**
Otázka	**Záznam**	**Predpokladané odpovede**
Názov budovy		Názov, prípadne adresa
Adresa budovy		
Názov areálu		Do ktorého budova patrí
Vlastník budovy		Kto je vlastník?
Počet vchodov, poschodí		Aj nevyužívané vchody
Počet organizácií v budove		
Umiestnenie v budove		Umiestnenie organizácie v budove
	Plášť budovy: MSZ	
Technické prvky PKB		Popisuje sa plášť budovy.

Zabezpečenie dverí		Konštrukcia dverí, bezpečnostné dvere?, osadenie dverí, mreže.
Zabezpečenie okien		Mreže?, bezpečnostné fólie? Konštrukcia, sú všade?
MSZ popis iné		Iné ak existuje popis.
	Plášť budovy: elektronické prvky PKB	
ACCESS popis		El. vrátnik?, turnikety, magnetické karty ? (popis systému).
CCTV popis		CCTV na plášti budovy, popis.
EZS popis		Senzory (PIR, mikrovlnné, duálne..a pod.)
EPS popis		Ak existujú.
	Vnútro budovy: MSZ	
Zabezpečenie dverí		Zabezpečenie dverí medzi zabezpečenými priestormi.
Zab. vnútorných priestorov		Prekážky, mreže, oddelenie vnútorných priestorov.
MSZ popis iné		
	Vnútro budovy: elektronické prvky PKB	
ACCESS popis		Medzi chránenými priestormi, magnetické karty? Prvky ACCESS popis.
CCTV popis		Rozmiestnenie popis, záznam, technický popis.
EZS popis		Rozmiestnenie PIR, druhy, technický popis, funkčnosť.
EPS popis		Ak sú rozmiestnenie popis, technický popis.
	Režimové opatrenia budova	
Kontrola vstupu		Smernice kontroly vstupu: preveruje sa obsah, kto kedy kam.
Kontrola pohybu osôb		Popis praxe: kto kde s kým kedy, doprovod?, obsah smerníc.
Kľúčový poriadok budovy		Obsah smerníc, prípadne popis procesov.
Prevádzkový por. budovy		Obsah dokumenty, prípadne popis procesov.
Smernica strážnej služby		Ak je k dispozícii.
Status požiarnej ochrany		Existencia, aktualizácia, revízie.
	Personálne opatrenia - budova	
Strážna služba		Ak je umiestnenie, popis činnosti.
Vrátnik		Na vstupe, existencia smerníc, popis činnosti.
Informátor a pod.		Dohľad nad pohybom osôb, popis činnosti.
Zodpovedné osoby pohyb		Návštevy, priradenie zodpovedností.
POZNÁMKY:		

Tabuľka 3: Príklad: formulár pre preskúmanie úrovne fyzickej bezpečnosti budovy.

Miesto popis IS	Spoločnosť:	Spracoval:
	X	**Daniel Bednárik**
Otázka	**Názov miesta**	**Nápoveda, možné odpovede**
	Spoločnosť:	
Pracovná stanica		Názov PC, NT, alebo interné označenie
Spracovávaná agenda		Ekonomická, PAM....
Názov IS		IS týkajúci sa OOÚ, keď nie je tak nie
Názov miestnosti		
Označenie miestnosti		Prípadne používaný názov
Označenie budovy		
Podlažie		
Počet vstupných dverí		
Monitor umiestnenie		Proti od pozeraniu
Stoly predmety		Šanóny, zmluvy, len používaná agenda
Písomná forma AIS		
Názov písomného AIS		V miestnosti len OOÚ
Typ úschovného zariadenia		skriňa, polica, trezor
Je uzamykateľné?		Áno/nie
Likvidácia dokumentov		Mechanická likvidácia, skartovanie
Technické prvky PKB		
Zabezpečenie dverí (MSZ)		Konštrukcia, bezp. dvere guľa, mreže
Zabezpečenie okien (MSZ)		Mreže, bezpečnostné fólie
ACCESS popis		El vrátnik, magnetický zámok
CCTV popis		V miestnosti
EZS popis		PIR +funkčnosť, typy, mg. Kont. Okná dvere
EPS popis		Typy, funkčnosť
Režimové opatrenia		
Kontrola vstupu		zamestnanci, externisti, návštevy, upratovačka
Kontrola pohybu osôb		Pod dohľadom?
Kľúčový poriadok budovy		Overuje sa písomná forma
Smernica strážnej služby		Ak je k dispozícii

Miesto popis IS	Spoločnosť:	Spracoval:
	X	**Daniel Bednárik**
Otázka	**Názov miesta**	**Nápoveda, možné odpovede**
Personálne opatrenia		
Počet oprávnených osôb		Počet osôb
Počet osôb celkom		Celkom všetkých osôb

Tabuľka 4: popis miesta (miesto pracovnej stanice), preskúmanie úrovne fyzickej bezpečnosti.

ISO AIS	Spoločnosť:	Spracoval:
	X	**Daniel Bednárik**
Otázka	**Záznam**	**Nápoveda, možné odpovede**
IS 1, názov		Ak je IS viacej rozdeľte stĺpec záznam
Spracovávaná agenda		
Zoznam informácií		Uviesť na konci formuláru
IS 2, názov		
Spracovávaná agenda		
Zoznam informácií		Uviesť na konci formuláru
IS 3, názov		
Spracovávaná agenda		
Zoznam informácií		Uviesť na konci formuláru
HW vrstva		
Popis kabeláže		Popis podľa vrstvy OSI (1 vrstva). Štruktúrovaná kabeláž, popis topológie štruktúrovanej kabeláže, popis technického spracovania (UTP, FTP) Je kabeláž realizovaná podľa platných noriem? (káblové chráničky, žľaby, lišty)
Sieťová vrstva		
Topológia siete popis		Popis topológie siete, rozdelenie, VPN a pod.
Internet/poskytovateľ		Typ pripojenia na internet, poskytovateľ pripojenia
Popis sieťových prvkov		Popis, podľa vrstiev OSI (2,3)
Sú monitorované?		Čo všetko je monitorované?

ISO AIS	Spoločnosť:	Spracoval:
	X	**Daniel Bednárik**
Otázka	**Záznam**	**Nápoveda, možné odpovede**
Je analyzovaná prevádzka siete?		Sú analyzované logy, činnosť používateľov?
Popis siete OSI (4,5,6,7)		Používané protokoly (7 vrstva), FTP, SMTP, IMAP a pod.)
HW Servery		Určenie, štruktúra serverov
Záložné zdroje?		
HW serverov		Architektúra, výrobcovia
Serverovňa popis		Je klimatizácia?
RO serverovňa		Popis režimových opatrení v serverovni, kľúčový režim, monitoring prístupu.
Aplikačná vrstva servery		
Aplikácie OOÚ názov, výrobca		Názov, architektúra, výrobca, aplikačné prostredie na ktorom beží.
Aktualizované aplikácie OOÚ		
Automaticky aktualizované?		
Súbory s dátami kryptované?		
Zabezpečenie SERVERY		
Typy OS		Napísať WXP Home,...
Aktualizované?		Je OS aktualizovaný?
Automatické aktualizácie?		Automaticky?
Firewall		Zapnutý?
Antivírusový program		Je?
Antivírový sv. aktualizovaný?		Aktualizovaný?
Aplikácie sú aktualizované?		Aktualizujú sa aplikácie? Ako?
Zálohovanie		
Popis hw zariadenia		Zálohovacieho zariadenia
Popis SW zariadenia		
Sú definovane dáta?		
Je definovaný interval		
Uskladnenie médií		Uskladnenie zálohovacích médií
Existuje evidencia záloh?		
Kontrolujú sa zálohy?		

ISO AIS	Spoločnosť:	Spracoval:
	X	**Daniel Bednárik**
Otázka	**Záznam**	**Nápoveda, možné odpovede**
Používanie hesiel		
Čo všetko vyžaduje heslo?		
Dĺžka hesiel		
Štruktúra hesiel		Zloženie hesiel
Cyklická zmena hesiel		
Popis ostatný		
Logy		Sú vytvárané logy? Čo sa loguje? Skúma ich niekto?
		Sú logy chránené
Monitorovanie		Čo sa monitoruje? Ako sa to monitoruje
Synchronizácia hodín		Ako sú hodiny synchronizované
Technická podpora		Existuje znalostná databáza riešenia problémov?

Tabuľka 5: posúdenie bezpečnosti informačného systému

ISO OSI miesto	Spoločnosť:	Spracoval:
	X	**Daniel Bednárik**
Otázka	**Názov 1**	**Nápoveda, možné odpovede**
Súvisiaci názov PC		Názov súvisiaceho PC, pracovná stanica
Popis HW		Technický stav a dostatočnosť systémových zdrojov
Typ		PC/Notebook
Architektúra		Intel, Linux, Mac
Procesor		Obecne typ
RAM		Veľkosť RAM
HDD		Veľkosť
BIOS heslo?		Áno/Nie
Monitor typ		LCD, CRT
Sieť		Áno/Nie
IP statická?		Áno/Nie

ISO OSI miesto	Spoločnosť:	Spracoval:
	X	**Daniel Bednárik**
Otázka	**Názov 1**	**Nápoveda, možné odpovede**
Prihlasovanie do siete		Áno/Nie
Zabezpečenie PC		
Typ OS		Napísať WXP Home,...
Updated?		Je OS aktualizovaný?
Automatické aktualiz.?		Automaticky?
Firemný		Zapnutý?
Antivírusový program		Je?
Antivír aktualizovaný?		Aktualizovaný?
Aplikácie aktualizované?		Aktualizujú sa aplikácie? Ako?
User is admin?		Či sa používateľ prihlasuje, ako administrátor
Prihlasovanie:		
Dĺžka hesla		Znaky
Zloženie hesla		Aké znaky?
Expirácia hesla		Periodická exspirácia
Šetrič obrazovky+heslo?		Spúšťa automaticky šetrič?
Periférie		
USB Flash aktívne?		Sú aktívne USB?
CDROM/DVD?		Áno/nie
Iné prenosné zariadenia?		Definovať
Tlačiarne		Áno/nie
Lokálna, sieťová?		Určiť
Zálohovanie PC		
Periodicita		
Zariadenie, nosič		
Čo sa zálohuje?		

Tabuľka 6: posúdenie bezpečnosti informačného systému: pracovná stanica

Porada, príprava pracovného tímu pozostáva z bodov:

- oboznámenie členov tímu s cieľom a účelom BP prieskumu,
- oboznámenie členov tímu zo stratégiou BP prieskumu,
- s metodikou BP prieskumu,
- s plánom a časovým rozvrhom BP prieskumu,
- oboznámenie členov tímu s informáciami získanými predbežným BP prieskumom,
- oboznámenie členov tímu s metodikou BP prieskumu,
- určenie rolí členov tímu a určenie bezpečnostných oblastí, ktoré budú skúmať,
- oboznámenie členov tímu s pravidlami vyplňovania tlačív a formulárov,
- preskúšania členov tímu,
- preverenia úplnosti všetkých potrebných dokumentov a technických prostriedkov.

4.4 Analýza rizík bezpečnosti informačného systému

Na základe informácií z bezpečnostného prieskumu bola vykonaná analýza rizík bezpečnosti informačného systému.

4.4.1.1 Nastavenie metrík hodnotenia výsledkov z bezpečnostného prieskumu

Hodnotenie identifikovaných aktív:

Aktívum je hodnotené z pohľadu narušenia:

Dostupnosti f(x), dôvernosti f(y), Integrity f(z) aktíva.

Hodnota aktíva:

- **Nízka f(x):** narušením dostupnosti, dôvernosti, integrity nevzniká finančná strata.
- **Stredná f(y):** krátkodobá nefunkčnosť systému, alebo zníženie jeho výkonu, finančné straty priame, alebo nepriame (v dôsledku) do 3000 €
- **Vysoká f(z):** právne postihy v dôsledku poškodenia, straty, neužitia informácií, ohrozenie chodu organizácie, vysoké finančné straty.

Váha hodnotenia aktíva je určená funkciou f= {f(x)+f(y)+f(z)}/3.

Kvalitatívne hodnotenie identifikovaných hrozieb:

- Nízka P > 0 = váha 1: daná hrozba využije zraniteľnosť aktíva len v veľmi malou pravdepodobnosťou, hraničiacou s nulou.
- Stredná P ≈ 0,5 = váha 2: pravdepodobnosť uskutočnenia hrozby je významná.
- Vysoká P < 1 = váha 3: je vysoko pravdepodobné sa hrozba uskutoční.

Výsledkom je určenie váh hrozieb pre jednotlivé identifikované aktíva, tieto váhy sú použité pre určenie miery rizika.

Poznámka: použité číselné vyjadrenie pravdepodobností je nastavením systému metriky vyjadrenia váhy hrozby pre ďalšie hodnotenie. Nevyjadruje okamžité reálne hodnoty pravdepodobností hrozieb existujúcich v danom časovom okamihu.

Hodnotenie úrovne implementácie prijatých bezpečnostných opatrení:

- neimplementované: 3
- implementované čiastočne, nízka efektivita: 2
- implementované: 1

Číselná hodnota je váha, ktorá je použitá v hodnotení rizík.

Hodnotenie rizík, nastavenie metriky:

Pre hodnotenie rizika sa použijú váhy hodnotenia z:

- hodnotenia aktív,
- hodnotenia hrozieb,
- hodnotenia úrovne implementácie prijatých bezpečnostných opatrení.

Váha rizika (miera rizika) = Váha hrozby x Váha zraniteľnosti, Vr= Vh*Vz

Aktívum /komponent	Zdroje aktíva	DS	DV	INT	Váha	HD
IS (CRM)	Softvér servera OSI 7 (CRM)	2	3	3	2,67	vysoká
	Operačný systém servera (CRM)	2	3	3	2,67	vysoká
	Hardvér servera (CRM)	2	3	3	2,67	vysoká
	Dáta servera (CRM)	2	3	3	2,67	vysoká
	Písomná forma (CRM)	2	3	3	2,67	vysoká
	Služba (CRM)	2	3	3	2,67	vysoká

Tabuľka 7: časť tabuľky hodnotenia aktív

Definícia miery rizika:

- nízka Vr = hodnoty váhy 2 a 1,
- stredná Vr = hodnoty váhy 4 a 3,
- vysoká Vr = hodnoty váhy 9 a 6.

Aktívum /komponent aktíva	Typ			Zdroje aktíva	
IS (CRM)	Softvér			Softvér servera OSI 7 (CRM)	
Identifikovaná hrozba	**Vh**	**Vz**	**Vr**	**Miera rizika**	**HD**
zemetrasenie	1	1	1	nízka	vysoká
povodeň	1	1	1	nízka	vysoká
víchrica	1	1	1	nízka	vysoká
bombový útok	1	1	1	nízka	vysoká
blesk	1	1	1	nízka	vysoká
priemyselná akcia	1	1	1	nízka	vysoká
požiar	1	1	1	nízka	vysoká
úmyselná škoda	2	2	4	**stredná**	vysoká
prerušenie dodávky el. energie	1	1	1	nízka	vysoká
prerušenie dodávky vody	1	1	1	nízka	vysoká
porucha klimatizácie	1	1	1	nízka	vysoká
porucha hardvéru	2	2	4	stredná	vysoká
kolísanie napájania	2	1	2	nízka	vysoká
extrémna teplota a vlhkosť	1	1	1	nízka	vysoká
prach	1	1	1	nízka	vysoká
elektromagnetická radiácia	1	1	1	nízka	vysoká
elektrostatický náboj	1	1	1	nízka	vysoká
krádež	3	1	3	**vysoká**	vysoká
neoprávnené použitie pamäťového média	3	2	6	**vysoká**	vysoká
poškodenie pamäťového média	3	3	9	**vysoká**	vysoká
chyba zamestnancov – chyba obsluhy	3	3	9	**vysoká**	vysoká
chyba údržby	2	1	2	**stredná**	vysoká
zlyhanie softvéru	-	-	0	x	vysoká
použitie softvéru neautorizovanými používateľmi	3	3	9	**vysoká**	vysoká
použitie softvéru neautorizovaným spôsobom	2	2	4	**stredná**	vysoká
predstieranie identity používateľa	2	1	2	**stredná**	vysoká
nelegálne používanie softvéru	3	2	6	**vysoká**	vysoká
počítačový vírus – škodlivý softvér	3	1	3	**vysoká**	vysoká
nelegálny import/export softvéru	2	1	2	**stredná**	vysoká
prístup k sieti neautorizovanými používateľmi	1	1	1	nízka	vysoká
neautorizované použ. sieťového vybavenia	1	1	1	nízka	vysoká
technické zlyhanie sieťových komponentov	1	1	1	nízka	vysoká
chyba prenosu	1	1	1	nízka	vysoká
poškodenie vedenia	1	1	1	nízka	vysoká
preťaženie	1	1	1	nízka	vysoká
odpočúvanie	1	1	1	nízka	vysoká
infiltrácia komunikácií	1	1	1	nízka	vysoká

analýza sieťovej prevádzky	1	1	1	nízka	vysoká
chybné smerovanie správ	1	1	1	nízka	vysoká
presmerovanie správ	1	1	1	nízka	vysoká
popretie	1	1	1	nízka	vysoká
zlyhanie komunikačných služieb	1	1	1	nízka	vysoká
nedostatok zamestnancov	1	1	1	nízka	vysoká
chyby používateľov	2	2	4	**stredná**	vysoká
nesprávne použitie zdrojov.	2	2	4	**stredná**	vysoká

Tabuľka 8: hodnotenie rizík: určenie miery rizika a hodnoty dopadu

	Hodnota dopadu		
Miera rizika	Nízka	Stredná	Vysoká
Nízka	**P3**	**P3**	**P2**
Stredná	**P3**	**P2**	**P1**
Vysoká	**P2**	**P1**	**P1**

Tabuľka 9: Priorita implementácie navrhovaných bezpečnostných opatrení.

4.5 Syntéza z bezpečnostného prieskumu

Boli identifikované a ohodnotené aktíva, hrozby, riziká, zraniteľnosti. Boli preskúmané jednotlivé bezpečnostné oblasti definované v štandarde STN ISO 27002 a to:

- bezpečnostné politiky,
- organizácia informačnej bezpečnosti,
- riadenie aktív,
- bezpečnosť ľudských zdrojov,
- fyzická bezpečnosť a bezpečnosť prostredia,
- riadenie komunikácie a prevádzky,
- riadenie prístupu,
- akvizícia, vývoj a údržba informačných systémov,
- riadenie incidentov informačnej bezpečnosti,
- riadenie kontinuity činnosti,
- súlad s technickými normami a právnymi predpismi.

4.5.1 Príklad 1: syntéza bezpečnostnej oblasti bezpečnostná politika informačnej bezpečnosti

Cieľom je poskytnúť usmernenie pre riadenie a podporu informačnej bezpečnosti v súlade s relevantnými zákonmi a nariadeniami. Politika informačnej bezpečnosti by mala byť súčasťou všeobecnej bezpečnostnej politiky.

4.5.1.1 Dokument politiky informačnej bezpečnosti

Dokument bezpečnostnej politiky by mal byť schválený Manažmentom, vydaný a oznámený všetkým zamestnancom, ako aj relevantným externým partnerom.

Popis stavu implementácie:

- Neexistuje dokument informačnej bezpečnosti.

Návrh opatrení: priorita implementácie P1 - vysoká

- Vytvoriť formálny dokument: bezpečnostná politika informačnej bezpečnosti, ktorý bude stanovovať angažovanosť manažmentu a vytyčovať prístup organizácie k riadeniu informačnej bezpečnosti, ktorý bude obsahovať:
- Definíciu informačnej bezpečnosti, jej celkové ciele, účel a dôležitosť bezpečnosti ako mechanizmu umožňujúceho spoločné používanie informácií.
- Vyhlásenie zámerov manažmentu, podpory cieľov a princípov informačnej bezpečnosti v súlade s podnikateľskou stratégiou a cieľmi.
- Rámec na nastavenie cieľov riadenia a opatrení, vrátane štruktúry preskúmavania rizík a riadenia rizík.
- Stručné vysvetlenie bezpečnostných politík, princípov, štandardov a zhody s požiadavkami, dodržiavanie ktorých má pre organizáciu zvláštnu dôležitosť:
    - dodržiavanie legislatívnych, regulačných a zmluvných požiadaviek,
    - požiadavky na bezpečnostné vzdelávanie, zácvik a budovanie bezpečnostného povedomia,
    - riadenie kontinuity činnosti organizácie,
    - následky porušení bezpečnostnej politiky.
- Definíciu všeobecných a špecifických zodpovedností z hľadiska manažmentu informačnej bezpečnosti, vrátane ohlasovania bezpečnostných incidentov.

- Odkazy na dokumentáciu, podporujúcu danú politiku, napr. detailnejšie bezpečnostné pravidlá a postupy pre špecifické informačné systémy alebo bezpečnostné pravidlá, ktoré by mali používatelia dodržiavať.

S touto politikou oboznámiť používateľov v rámci celej organizácie, a to formou, ktorá je patričná, dostupná a pochopiteľná pre očakávaného čitateľa.

4.5.1.2 Preskúmanie politiky informačnej bezpečnosti

Politika informačnej bezpečnosti by mala byť preskúmavaná v plánovaných intervaloch, ako aj okamžite pri výskyte významných zmien, čím sa zabezpečí jej kontinuálna vhodnosť, primeranosť a efektivita.

Popis stavu implementácie:

- Keďže neexistuje oficiálna politika informačnej bezpečnosti, nemôže byť ani preskúmavaná.

Návrh opatrení: priorita implementácie P1 - vysoká

- Definovať politiku informačnej bezpečnosti.
- Vytvoriť formálny dokument politiky informačnej bezpečnosti.
- Priradiť zodpovednú osobu za politiku informačnej bezpečnosti, ktorý akceptoval Manažérsku zodpovednosť za jej vývoj, revíziu a vyhodnocovanie efektivity.
- Určiť postupy, metódy, intervaly, harmonogramy preskúmavania primeranosti politiky informačnej bezpečnosti za účelom jej revízie.
- Určiť postupy, metódy, intervaly, harmonogramy preskúmavania efektivity implementácie politiky informačnej bezpečnosti. (riadiaca činnosť manažmentu)

4.5.2 Príklad 2: syntéza bezpečnostnej oblasti: bezpečnosť ľudských zdrojov

4.5.2.1 Proces preverovania pred nástupom do zamestnania

Mala by sa vykonať verifikačná previerka personálneho pozadia všetkých uchádzačov o zamestnanie, zmluvných partnerov a používateľov v pozícii tretích strán v súlade s príslušnými zákonmi, právnymi nariadeniami a etikou, ako aj vzhľadom na obchodné požiadavky, klasifikačný stupeň informácií, ku ktorým sa bude pristupovať, ako aj na vnímané riziká.

Popis stavu implementácie:

- Personálnym oddelením sú vykonávané verifikačné previerky, berú do úvahy všetky zákony zaoberajúce sa ochranou súkromia, ochranou osobných údajov a ostatných právnych predpisov súvisiacich s procesom zamestnávania.

Návrh opatrení: žiadne

4.5.2.2 Role a zodpovednosti

Popis stavu implementácie:

- Bezpečnostné role a zodpovednosti zamestnancov, zmluvných partnerov a používateľov v pozícii tretích strán sú neformálne definované.

Návrh opatrení: priorita implementácie P1 - vysoká

- Definovať bezpečnostné role a zodpovednosti v súlade s formálnou politikou informačnej bezpečnosti organizácie.
- Definícia bezpečnostnej roly by mala obsahovať:
- Spôsob implementácie bezpečnostnej roly do systému riadenia informačnej bezpečnosti .
- Definíciu ochrany aktív pred neautorizovaným prístupom, prezradením, modifikáciou, zničením alebo neoprávneným zásahom.
- Výkon špecifických bezpečnostných procesov a činností pre rolu.
- Zabezpečenie pridelenia zodpovednosti konkrétnej personálnej zodpovednosti osobe za svoje konanie.
- Definovať spôsob oznamovania bezpečnostných udalostí, resp. potenciálnych udalostí alebo iných bezpečnostných rizík organizácie.
- Určiť spôsob oboznámenia sa príslušnej osoby s povinnosťami výkonu bezpečnostnej role, tak aby bolo oboznámenie zrozumiteľné. (riadiaca činnosť manažmentu)

4.5.2.3 Pracovná náplň a podmienky zamestnania

Ako súčasť ich záväzkov vyplývajúcich zo zmluvy by zamestnanci, zmluvní partneri a používatelia v pozícii tretích strán by mali odsúhlasiť a podpísať zmluvu o pracovnej náplni a podmienkach zamestnania definujúcu aj ich zodpovednosť týkajúcu sa informačnej bezpečnosti.

Popis stavu implementácie:

- V zmluvách zo zamestnancami je definovaná zodpovednosť týkajúca sa informačnej bezpečnosti .

Návrh opatrení: žiadne opatrenia

4.5.2.4 Manažérske zodpovednosti

Manažment by mal od zamestnancov, zmluvných partnerov a používateľov v pozícii tretích strán vyžadovať uplatňovanie bezpečnosti v súlade so zavedenými politikami a procedúrami organizácie.

Popis stavu implementácie:

- Zamestnanci, zmluvní partneri a používatelia v pozícii tretích strán:
- Nie sú oboznámení o ich rolách a zodpovednostiach spojených s informačnou bezpečnosťou ešte predtým, ako im bol udelený prístup k citlivým informáciám a informačným systémom.
- Nie sú im poskytnuté formálne usmernenia pojednávajúce o tom, čo sa od nich očakáva z hľadiska výkonu ich bezpečnostnej roly v organizácii.
- Dosahujú určitú úroveň bezpečnostného povedomia potrebného na výkon ich rolí a zodpovednosti v organizácii.
- Podriaďujú sa pracovnej náplni a podmienkam zamestnania.

Návrh opatrení: priorita implementácie P1 - vysoká

- Poučiť zamestnancov o ich rolách a zodpovednostiach spojených s informačnou bezpečnosťou.
- Zamestnancov oboznámiť zo smernicami, týkajúcimi sa informačnej bezpečnosti .
- Neustále motivovať zamestnancov k napĺňaniu bezpečnostných politík organizácie.
- Neustále zvyšovať úroveň bezpečnostného povedomia potrebného na výkon ich rolí a zodpovednosti v organizácii.
- Neustále zvyšovať úroveň dostatočných zručnosti a kvalifikácie.

4.5.2.5 Povedomie o informačnej bezpečnosti, vzdelávanie a školiaca činnosť

Všetci zamestnanci organizácie a v prípade, že je to potrebné aj zmluvní partneri a používatelia v pozícii tretích strán by mali absolvovať vhodné školenie v oblasti bezpečnostného povedomia a mali by im byť poskytované pravidelne aktualizované verzie politík a procedúr organizácie, tak ako si to vyžaduje ich pracovné zaradenie.

Popis stavu implementácie:

- Neprebieha školenie bezpečnostného povedomia, nie je definovaná periodicita školení.

Návrh opatrení: priorita implementácie P1 – vysoká:

- Vypracovať osnovu školenia bezpečnostného povedomia vzťahujúcej sa k problematike informačnej bezpečnosti.

4.5.2.6 Disciplinárny proces

Mal by existovať disciplinárny proces pre zamestnancov, ktorí spôsobili porušenie bezpečnosti.

Popis stavu implementácie:

- Existuje disciplinárny proces porušenia informačnej bezpečnosti pre zamestnancov.

Návrh opatrení: žiadne

4.5.2.7 Zodpovednosti v súvislosti s ukončením pracovnoprávneho pomeru

Zodpovednosti za realizáciu zrušenia pracovného pomeru alebo za zmenu jeho podmienok by mali byť jasne definované a pridelené.

Popis stavu implementácie:

- Sú pridelené zodpovednosti, definované postupy v prípade zrušenia pracovnoprávneho vzťahu, alebo inej zmluvy.

Návrh opatrení: žiadne

4.5.2.8 Vrátenie aktív, odňatie prístupových práv

Všetci zamestnanci, zmluvní partneri a používatelia v pozícii tretích strán by mali vrátiť akékoľvek aktíva patriace organizácii po ukončení ich pracovného pomeru, vypršaní uzatvorenej dohody alebo prevádzkovej zmluvy.

Popis stavu implementácie:

- Proces výpovede, ukončenia zmluvy je formalizovaný tak aby zahŕňal aj vrátenie predtým používaného softvéru, podnikových dokumentov, mobilné výpočtové

zariadenia, prístupové karty, manuály a informácie uchovávané na elektronických médiách.

Návrh opatrení: žiadne opatrenia

	Bezpečnostn	Bezpečnostné	Bezpečnostné	Priorita	Riešiteľ	Spôsob riešenia	Ch	Usmernenie i
1	5 Bezpečnostná politika	5.1 Politika informačnej bezpečnosti	5.1.1 Dokument politiky informačnej bezpečnosti	Vysoká	Menežment	Schváliť, upraviť navrhovaný dokument bezpečnostnej politiky orgnanizácie.	☑	Dokument bezpečnostnej politiky by mal byť schválený manažmentom, vydaný a oznámený všetkým
2	5 Bezpečnostná politika	5.1 Politika informačnej bezpečnosti	5.1.1 Dokument politiky informačnej bezpečnosti				☐	Dokument bezpečnostnej politiky by mal byť schválený manažmentom, vydaný a oznámený všetkým
3	5 Bezpečnostná politika	5.1 Politika informačnej bezpečnosti	5.1.2 Preskúmanie politiky informačnej bezpečnosti	Vysoká	Určená osoba	Adekvátnosť politiky informačnej bezpečnosti preskúmavať v pravidelných intervaloch.	☑	Politika informačnej bezpečnosti by mala byť preskúmavaná v plánovaných intervaloch, ako aj okamžite
4	5 Bezpečnostná politika	5.1 Politika informačnej bezpečnosti	5.1.1 Dokument politiky informačnej bezpečnosti	Vysoká	Menežment, určená osoba	Oboznámiť užívateľov v organizácii bežným spôsobom s bezpečnostnou politikou.	☑	Dokument bezpečnostnej politiky by mal byť schválený manažmentom, vydaný a oznámený všetkým
5	5 Bezpečnostná politika	5.1 Politika informačnej bezpečnosti	5.1.1 Dokument politiky informačnej					Politika informačnej bezpečnosti by

Obrázok 10: softvéru pre návrh bezpečnostných opatrení pre kontrolný zoznam.

Navrhované bezpečnostné opatrenia kontrolný zoznam

Bezp. kategória	Bezpečnostné opatrenie	Priorita	Riešiteľ	Spôsob riešenia	Dátum prijatia
10.1 Prevádzkové postupy a zodpovednosti	10.1.1 Dokumentované prevádzkové postupy	Vysoká	Menežment	Zaviesť navrhnuté smernice pre prácu a správu informačného systému. Definovať procedúry reštartovania systému a procedúry zotavenia. Určiť	
10.4 Ochrana proti škodlivému softvéru	10.4.1 Opatrenia proti škodlivému kódu	Vysoká	IT správca	Zaviesť navrhované smernice pre prácu s informačným systémom. Pripraviť primerané plány kontinuity činnosti organizácie.	
10.5 Zálohovanie	10.5.1 Zálohovanie informácií	Vysoká	Menežment	Zaviesť navrhované smernice pre zálohovanie.	
10.7 Manipulácia s médiami	10.7.2 Likvidácia médií	Vysoká	Menežment	Schváliť navrhovanú smernicu pre likvidáciu úložných médií.	
11.1 Požiadavky na riadenie prístupu	11.1.1 Politika riadenia prístupu	Vysoká	Menežment	Zaviesť navrhovanú smernicu pre pravidlá riadenia prístupu a práva každého používateľa alebo skupiny používateľov.	
11.2 Riadenie prístupu	11.2.1 Registrácia používateľov	Vysoká	Menežment	Zaviesť formálnu procedúru registrácie a deregistrácie	

Obrázok 11: výstupná zostava: kontrolný zoznam navrhovaných opatrení pre organizáciu.

ZÁVER

Bezpečnostný prieskum je náročný proces z pohľadu odbornosti, plánovania a riadenia procesu, z pohľadu zabezpečenia ľudských zdrojov, výberu vhodných metodík bezpečnostného prieskumu. Je ťažké odhaliť všetky hrozby, popísať všetky procesy, súvislosti, vyhľadať zraniteľnosti a navrhnúť primerané bezpečnostné opatrenia. Cieľom tejto diplomovej práce je bezpečnostným špecialistom nahradiť prípadný nedostatok praxe návodom pre realizáciu bezpečnostného prieskumu štruktúrovaným, formalizovaným a organizovaným prístupom.

ZÁVER V ANGLIČTINE

Security survey is a demanding process in terms of expertise, planning and management process in terms of providing human resources, selection of appropriate methodologies for research on security. It is difficult to detect all threats to describe all the processes, relationships, find vulnerabilities and propose appropriate safety measures. The aim of this thesis is a security specialist compensate for any lack of practical guidance for implementation of security research in a structured, formalized and organized approach.

ZOZNAM POUŽITEJ LITERATÚRY

1. **LAUCKÝ, V.** *Řízení technologických procesů v PKB.* Zlín : Academia centrum UTB, 2004.

2. **Milton D. Rosenau, Jr.** *Řízení projektů.* Brno : Computer Press, 2003. ISBN 80-7226-218-1.

3. **Broder, James F.** *Risk Analysis and Security Survey.* Burlington, MA 01803, USA : Butterworth-Heinemann is an imprint of Elsevier, 2006. ISBN 13: 978-0-7506-7922-0.

4. **LAUCKÝ, V.** *Technologie komerční bezpečnosti II.* Zlín : Academia centrum UTB, 2004.

5. **Černý, Vojtěch.** *Prodejní techniky.* Brno : Computer Press, 2003. ISBN 80-251-0032-4.

6. **Šimák, Ladislav.** MANAŽMENT RIZÍK. [Online] 2006, Žilina. [Dátum: 08. 04 2011.] http://www.scribd.com/doc/7337996/Manazment-rizik.

7. **LAUCKÝ, V.** *Bezpečnostní futurologie.* Zlín : Academia centrum UTB, 2007.

8. **ENISA - European Network and Information Security Agency.** enisa.europa.eu. [Online] 22. december 2010. [Dátum: 30.1.. január 2011.] http://www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide-in-slovak. WP2006/5.1(CERT-D1/D2).

9. *STN ISO/IEC 27001: 2005 Informačné technológie, zabezpečovacie techniky, systémy manažérstva informačnej bezpečnosti: požiadavky.* Bratislava : Slovenský ústav technickej normalizácie, 2006.

10. *STN ISO/IEC 27002: 2005 Informačné technológie, zabezpečovacie techniky, pravidlá dobrej praxe manažérstva informačnej bezpečnosti.* Bratislava : Slovenský ústav technickej normalizácie, 2006.

11. *STN ISO/IEC TR 13335-3.* Bratislava : Slovenský ústav technickej normalizácie, 2002.

12. **LAUCKÝ, V.** *Speciální bezpečnostní technologie.* Zlín : Academia centrum UTB, 2009.

13. **Zeman, Petr.** *Česká bezpečnostní terminologie.* Brno : Masarykova univerzita, 2002. ISBN 8O-210-3O37-2.

14. **MIKOLAJ, J.– HOFREITER, L. – MACH, V. – MIHÓK, J. – SELINGER.** *Terminológia bezpečnostného manažmentu, Výkladový slovník.* Košice : Multiprint s.r.o., 2004. ISBN 80-969148-1-2.

15. **Hurta, J. Laucký, V.** *Management bezpečnostního inženýrství.* Zlín : Zlín : Univerzita Tomáše Bati, 2006, 2006. 80-7318-412-5.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

BP prieskum	Bezpečnostný prieskum
TP PKB	Technické prostriedky priemyslu komerčnej bezpečnosti

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK