Bezpečnost informací v softwarech krizového řízení.

The information security to software of crisis management.

Ing. Martin Ficek - Univerzita Tomáše Bati ve Zlíně, nám. T. G. Masaryka 5555, 760 01 Zlín
E-mail: ficek@fai.utb.cz

prof. Mgr. Roman Jašek, Ph.D. - Univerzita Tomáše Bati ve Zlíně, nám. T. G. Masaryka 5555, 760 01 Zlín E-mail: jasek@fai.utb.cz

Abstrakt:

Tento článek se zabývá bezpečností informací v softwarech krizového řízení. Definuje typy informací v krizovém řízení a kategorizuje je dle potřeby ochrany.

Následně se zabývá samotnými softwary krizového řízení. Zde definuje šest oblastí podle určení příslušných softwarů a zabývá se vztahem mezi těmito softwary a informacemi. Určuje, druhy softwarů dle jejich práce s informacemi.

Článek využívá metodikou COBIT, COBIT kostkou a v omezené míře SWOT analýzu. Jednotlivé prvky COBT kostky jsou rozebrány a aplikovány do problematiky softwarů krizového řízení.

Vztahy mezi jednotlivými prvky COBIT kostky jsou demonstrovány prostřednictvím příkladů z aplikace COBIT kostky na problematiku softwaru krizového řízení a znázorňuje tím jisté obtíže a problémy spojené s touto problematikou.

Klíčová slova: COBIT, krizové řízení, software, informace, bezpečnost.

Abstract:

This paper deals with security of information in crisis management softwares. The paper defines types of information in the crisis management and categorizes these according to the needs of protection.

In the next part it deals with the crisis management software itself. The paper defines sixt areas according to determination of the appropriate software and engages in relation between these softwares and information. The paper specifies what software works with what information.

The paper works with COBIT methodology, COBIT cube and up to some extent with SWOT analysis. There are discussed particular elements of the COBIT cube and they are applied to the problematics of the crisis management software.

The paper demonstrates relations between particular elements of the COBIT cube through examples of the application of the COBIT cube to the problematics of the crisis management software and shows difficulties and problems associated with this.

Keywords: COBIT, crisis management, software, information, security

Úvod

S jakými informacemi se v krizovém řízení pracuje? Jaké informace jsou relevantní pro softwary krizového řízení? Jak jsou informace chráněny? Na tyto otázky se snaží článek najít odpověď.

Článek se bude zabývat klasifikací informací, manipulací s informacemi a jejich ukládáním, vše bude zaměřeno na oblast krizového řízení ve státní správě a specifikuje se na oblast softwarů určených pro krizové řízení.

Je třeba si úvodem říci, že i takto specifikovaná oblast je dosti široká a přestože se článek v následujících stranách bude snažit popsat celou rovinu dané problematiky, může se stát, že budou opomenuty určité aspekty či oblasti této problematiky. Ne však proto, že by autoři nechtěli, nebo opomněli dané aspekty či oblasti zahrnou, ale zkrátka proto, že by byl článek natolik obsáhlý, že by se ztratil jeho základní význam, jenž spočívá ve stručném shrnutí dané problematiky.

Informace v krizovém řízení

V úvodu této části je třeba poznamenat, že v oblasti krizového řízení ve státní správě a samosprávě se vyskytují informace zařazené do zvláštního režimu. Jedná se o informace utajované (vyhrazené) a informace citlivé.

Utajovanými informacemi, se v případě softwarů využívaných v krizovém řízení moc zabývat nebudeme. Přesto definice vyhrazených informací je. *„Vyhrazené informace jsou informace, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.“*[1]

Další kategorií, jak již bylo zmíněno, jsou informace citlivé. Obecně se jedná o: „neveřejnou informaci, která vyžaduje ochranu, protože její neoprávněné zveřejnění, použití, změna, ztráta nebo zničení by mohlo způsobit škodu osobě či instituci, jíž se týká. Základními kategoriemi citlivých informací jsou osobní údaje (např. zdravotní stav), ekonomické údaje (obchodní, průmyslové, služební, bankovní aj. tajemství) a údaje důležité pro bezpečnost státu (státní tajemství, utajované skutečnosti).“[2]

Tyto citlivé informace můžeme dále rozdělit na:

1) Skutečnosti, na které se vztahuje povinnost mlčenlivosti.
2) Osobní údaje - Chráněné dle zák. č. 101/2000 Sb., o ochraně osobních údajů.
3) Zvláštní skutečnosti - Chráněné dle zák. č. 240/2000 Sb., krizový zákon.

Co se týče specifických informací v softwarech krizového řízení, můžeme informace dělit na:

1) Informace grafické.
2) Informace psané.
3) Informace zvukové.

Jedná se o různé informace v digitální podobě například o mapové podklady, psané zprávy, hlasové záznamy a tak dále.

Z obecných informací krizového řízení jsou poté vybrány relevantní informace pro dané softwary.

Tato část měla sloužit jako základní uvedení do problematiky informací v krizové řízení.

Softwary krizového řízení

Softwarů, jež využívá krizové řízení, je celá řada neboť i problematika krizového řízení je dosti široká.

Pomineme-li softwary administrativního charakteru, jakými jsou například účetní systém, zbydou softwary specializované pro potřeby krizového řízení a softwary využitelné pro potřeby krizového řízení.

Například softwary Aloha, Terex, Posim, Obnova, IVVS, Argis, atd.

Pro přehlednost je můžeme dělit do několika skupin dle jejich zaměření a použití, jsou to:

1) Geografické informační systémy.
2) Systémy modelování a simulaci.
3) Systémy monitorovací.
4) Komunikační systémy.
5) Speciální databáze KŘ.
6) Další.

Přestože je toto dělení dosti zjednodušující, pro pochopení podstaty věci je to dostačující.

Typy softwarů krizového řízení a vztah k informacím.

V této části bude popsán typ informací, jimiž se jednotlivé druhy softwary krizového řízení zabývají. Je třeba říci, že každý z těchto systémů pracuje s databázemi, nicméně v oblasti krizového řízení existují i zvláštní databázové systémy a proto jsou uvedeny jako zvláštní skupina.

Geografické informační systémy – Tyto systémy pracují s grafickými informacemi (mapové podklady, obrázky a další), písemnými (informace v databázi, například polohy úkrytů, skaldů civilní ochrany atd.) a některé systémy i zvukovými informacemi.

Systémy modelování a simulaci – Tyto systémy pracují s grafickými informacemi (mapové podklady, obrázky a další), písemnými (informace nutné k vlastnímu modelování a simulaci např. postupy složek IZS, informace získané z měřících stanic etc.) a některé systémy i zvukovými informacemi (např. nahrané zvukové oznámení atd.).

Systémy monitorovací - Tyto systémy pracují s grafickými informacemi (obrázky, záznamy z kamer a další), písemnými (informace získané z měřících stanic či informace získané měřením a zapsané do systému atd.).

Komunikační systémy - Tyto systémy pracují s grafickými informacemi (obrázky, záznamy z kamer a další přenášené grafické informace), písemnými (nejrůznější přenášené písemné informace) a samozřejmě zvukovými informacemi (přenos hlasu, zvukových záznamů a podobně).

Speciální databáze krizového řízení - Tyto systémy pracují s grafickými informacemi (Grafické informace nutné pro fungování a efektivnost daného systému), písemnými

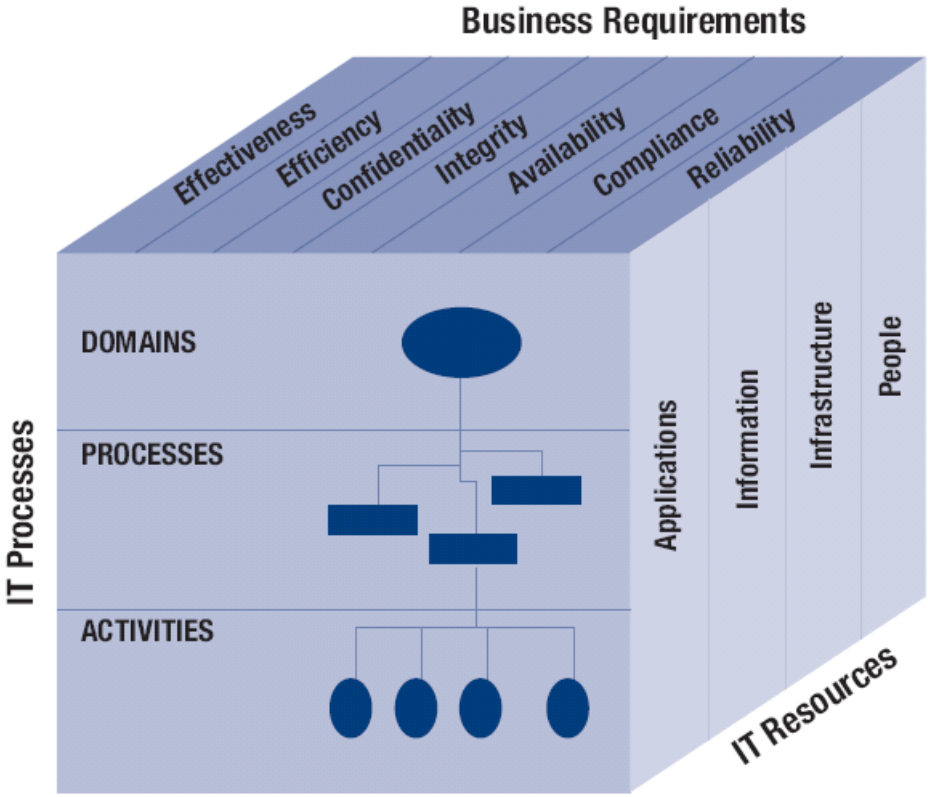
(informace v databázi, například polohy úkrytů, skaldů civilní ochrany, počty jednotek, vybavenost jednotek, atd.) a některé systémy i zvukovými informacemi.

Další - Tyto systémy pracují s grafickými informacemi (mapové podklady, obrázky a další), písemnými (informace v databázi, například rozhodnutí hejtmana, nařízení vedoucích pracovníků, atd.) a některé systémy i zvukovými informacemi.

Metodika COBIT

Pro potřeby tohoto článku bude použita metodika COBIT tedy Control Objectives for Information and Related Technology. *„Jedná se o sadu všeobecně přijímaných procesů, návodů pro hodnocení, ukazatelů a nejlepších praktických zkušeností, která má za cíl organizaci maximalizovat užitek plynoucí z informačních technologií.“*[3]

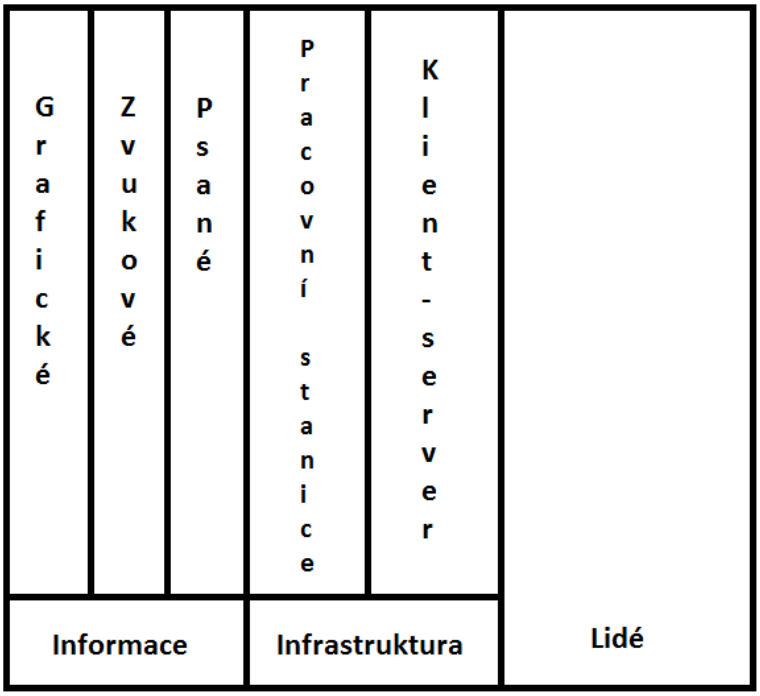
Základ této metodiky tvoří nástroj zvaný COBIT kostka. Tento nástroj pracuje s cíli organizace (strategické požadavky), zdroji informačních technologií a procesy.



Obrázek 1: COBIT kostka.[4]

Zdroje v softwarech krizového řízení

Základními zdroji jsou aplikace, informace; infrastruktura a lidé. Definujeme-li zdroje, je třeba si uvědomit, samy softwary jsou aplikacemi. Z tohoto důvodu leze zdroj aplikací vynechat. Jelikož hovoříme v obecné rovině, pak lze v bodě informací pouze shrnout, že máme informace grafické, informace psané, informace zvukové. Co se týče infrastruktury, zde se soustředíme především na hardware a distribuci samotného softwaru, tedy zda se jedná o software fungující na principu klient-server, nebo se jedná o software fungující na pracovní stanici. Poslední rovinou jsou lidé, kteří významným způsobem zasahují do oblasti bezpečnosti.



Obrázek 2: Strana zdrojů z COBIT kostky. Zdroj: Vlastní.

Pro lepší pochopení problematiky zdrojů zde bude využita SWOT analýza, která definuje silné a slabé stránky, příležitosti a ohrožení.

Tabulka 1: SWOT analýza zdrojů v SW v KŘ. Zdroj: Vlastní.

SWOT	**Pomocné**	**Škodlivé**
Vnitřní původ (vychází ze samotného softwaru a jeho prostředí)	Silné stránky: Vyšší zabezpečení místností s příslušnými pracovními stanicemi.	Slabé stránky: Nižší gramotnost pracovníků ve smyslu bezpečnosti a informací.
Venkovní původ	Příležitosti:	Ohrožení:

(vlivy, které nevychází z softwaru a jeho prostředí)	Využití moderních technologií	Blackout.

Jelikož je SWOT analýza určena jen pro demonstraci některých vybraných aspektů není třeba ji podrobněji rozebírat ani ji vyčíslovat.

Informační kritéria

Základními informačními kritérii jsou efektivnost, výkonnost, důvěrnost, integrita, dostupnost, shoda, hodnověrnost.

Hovoříme-li o efektivnosti, máme na mysli kritérium užitečnosti, tedy to jak je daný software, či jednotlivý proces prospěšný pro plnění daného úkolu. Ve většině případů v této oblasti je myšleno jak relevantní informace je software schopen poskytnout.

Kritériem výkonnosti je této oblasti převážně myšlena doba za jakou je software schopen zpravovat zadané informace a poskytnout výstup.

Kritériem důvěrnosti je částečně myšlena samotná bezpečnosti, jedná se zde totiž o schopnost softwaru poskytovat správné a vhodné informace. Zde je významný podíl bezpečnosti, neboť pouze je-li software dostatečně zabezpečen, může správně pracovat bez obav z napadení a z toho vyplývajícího znehodnocení dat.

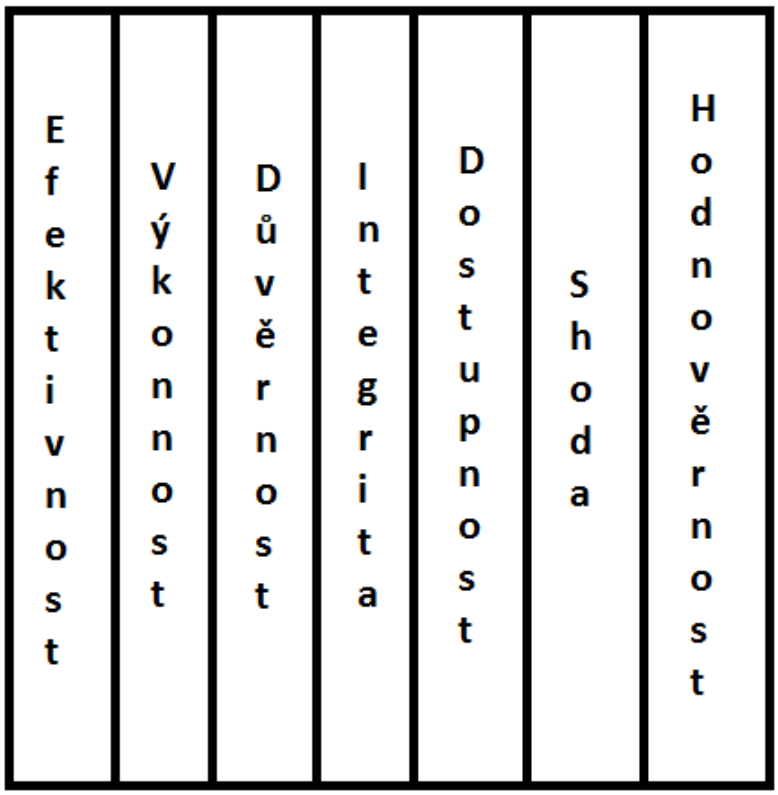
Pouze je-li dodržena integrita celého systému, může správně a plně fungovat, z tohoto důvodu se toto kritérium řadí mezi jeny z nejvýznamnějších.

Dostupnost, tento parametr je do značné míry ovlivněn formou softwaru a určením samotného softwaru, je jasné, že u komunikačního softwaru je dostupnost významnějším parametrem, než u GIS softwaru. Zde si ovšem musíme uvědomit, že dostupnost není jen parametr celého softwaru či informací, ale jednotlivých částí softwaru, to úzce souvisí s kritériem integrity.

Shoda je kritérium, které můžeme chápat jako poměr mezi záměrem, projektem a skutečností. Nestává se často, že je tento poměr 100%. Může být obtížné dosáhnout shody mezi záměrem a projektem (procesy), a ještě těžší bývá dosáhnout shody mezi projektem a

skutečností. Zde projekt vnímáme jako navržený systém nicméně ještě nezrealizovaný tedy teoretický.

Hodnověrnost, tak jako každý z výše popsaných parametrů, lze i tento parametr aplikovat, jak na jednotlivé části systému, tak na systém jako celek, či jeho zdroje a procesy, nicméně nejvyšší význam tohoto parametru je u výstupních informací. V praxi se například stává, že dva softwary pro modelování a simulaci dojdou k diametrálně rozdílným výsledkům.[1] Taková věc je dosti nepříjemná. Má-li krizový pracovník rozhodnout o rozsahu evakuace, potřebuje hodnověrné informace a proto je toto kritérium u softwarů používaných v krizovém řízení dosti zásadní obzvláště u výstupních informací.[6]



Obrázek 3: Strana kritérií z COBIT kostky. Zdroj: Vlastní.

IT procesy

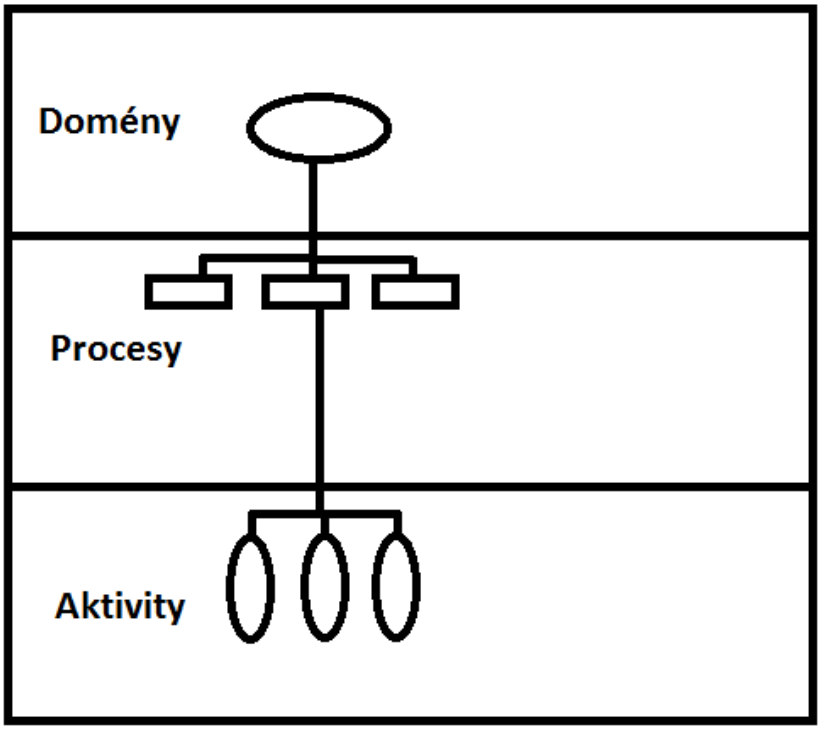
IT procesy jsou nejsložitějším prvkem, který je velmi složité definovat. IT procesy se skládají z domén, procesů a aktivit. Nejobecněji lze určit domény, zde se jedná

[1] Jak je například uvedeno v: FICEK, Martin, Dušan VIČAR, Jakub RAK a Petr SVOBODA. Using the SW modeling and simulating tools in transport of hazardous cargos na konferenci. In: TRANSPORT MEANS 2016. Juodkrante, Lithuania: Kaunas university of technology, 2016, s. 862-865. ISSN 2351-7034.

o plánování a organizaci, akvizici a implementaci, dodávku a podporu, a sledování a hodnocení.[3]

Domény poté využívají procesů, které využívají aktivit. Procesů a aktivit je v metodice COBIT definována celá řada a pro potřeby tohoto článku by bylo zatěžující se jimi zabývat.

Jelikož zde mluvíme o několika typech softwarů, není jednoduché určit přesné procesy a aktivity. Obecně lze tvrdit, že se bude jednat o procesy: ukládání informací, práce s informacemi, zobrazování, přenos dat, vkládání informací etc. Pochopitelně by bylo možné nalézti více procesů, nicméně pro ilustraci to stačí. Tyto procesy jsou dále rozděleny do aktivit.



Obrázek 4: Strana IT procesů z COBIT kostky. Zdroj: Vlastní.

Kostka COBIT

V této části článku budou výše popsané zdroje, kritéria a procesy aplikovány a znázorněny pomocí COBIT kostky. Je dobré si uvědomit, že zdroje jsou řízeny procesy tak, aby bylo dosaženo cílů, jež odpovídají daným kritériím.[5] [6]

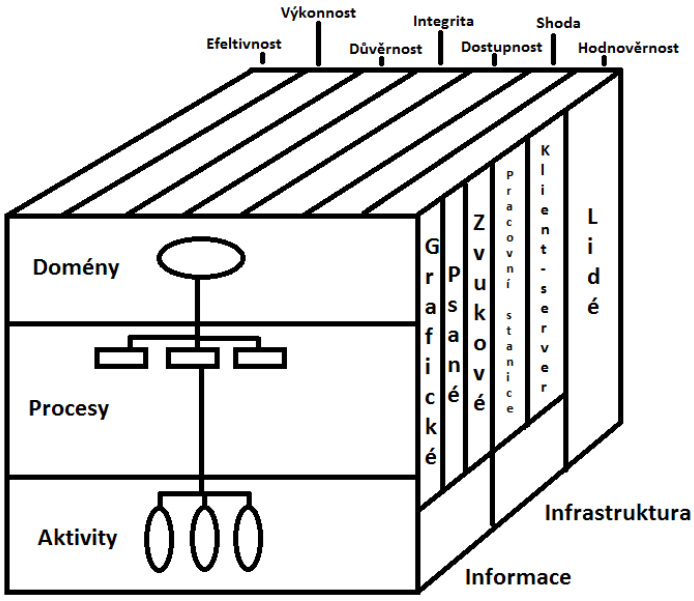
Aby bylo dosaženo, co nejlepšího stavu je třeba aplikovat v každá doméně adekvátní procesy a aktivity, jež budou pracovat se zdroji, tedy v tomto případě s informacemi ať již grafickými, psanými či zvukovými, infrastrukturou, ať již na principu pracovní stanice či klient-

server, a lidskými zdroji, tak aby výsledné cíle byli v souladu s kritérii, tedy efektivností, výkonností, důvěrností, integritou, dostupností, shodou a hodnověrností. [7] [8] [9]

Zjednodušeným příkladem pro vysvětlení může být například doména akvizice a implementace, v této doméně se mimo jiné nacházejí procesy pořizování softwaru, jeho implementace, sběr relevantních dat, jejich třídění a následné vložení do podniku, ale také školení pracovníků a jiné. Tyto procesy poté rozvíjejí další aktivity, například při procesu sběr relevantních dat budou například použity aktivity, získávání informací od odborníků, sběr dat od široké veřejnosti, sběr dat z nejrůznějších registrů atd. Při tomto kroku získáváme zdroj informace, ale také s informacemi jako zdrojem pracujeme (příkladem může být, práce s informacemi v podobě seznamu odborníků, na které se obrátíme atd.) využíváme zdroj infrastruktura (databáze mohou být naše vlastní např. seznam odborníků v podobě excelové tabulky, tedy na pracovní stanici, tak centrální registry na principu klient-server) a v neposlední řadě se zdrojem lidským. [10] [11]

Tyto zdroje v rámci procesů a aktivit řídíme tak, aby co nejvíce splňovaly kritéria. Příkladem může být kritérium efektivnosti při procesu sběru informací aktivitě zisk informací od odborníků. Zde budeme používat efektivně relevantní informace, takže místo seznamu úkrytů využijeme seznam odborníků, což jak jistě uznáte, bude více efektivní. Jelikož již takovýto seznam máme zhotoven a uložen na pracovní stanici, tak budeme využívat právě pracovní stanici a nikoli infrastrukturu klient-server, na které běží např. centrální registry, a musely bychom jednotlivé odborníky vyhledávat. Jak jistě uznáte i tento postup je efektivnější. V neposlední řadě ke sběru využijeme kvalifikované pracovníky pro takovýto úkon, například referenta krizového řízení, který má znalosti a schopnosti pro sběr požadovaného typu informací. I toto je efektivnější.

Je pochopitelné, že ve skutečnosti je celá problematika složitější, ale pro pochopení dané problematiky postačí tyto příklady.



Obrázek 5: Výsledná COBIT kostka. Zdroj: Vlastní.

Závěr

Díky obecnému směřování tohoto článku je náročné určit jednoznačnou míru bezpečnosti informací v softwarech krizového řízení. Je třeba říci, že současné softwary krizového řízení jsou již zabezpečeny na vysoké úrovni, ale vždy je co zlepšovat, ostatně jak ukazuje i metoda PDCA (plánuj, dělej, kontroluj, jednej), na jejímž základě je většina metodik postavena.

Tento článek se zabývala bezpečnosti informací v softwarech krizového řízení. Byly specifikovány informace v krizovém řízení a kategorizovány dle jejich potřeby zabezpečení na skutečnosti, na které se vztahuje povinnost mlčenlivosti, osobní údaje, zvláštní skutečnosti a na informace utajované. Dále se rozdělili informace dle formy a to na informace grafické, informace psané, informace zvukové.

Byly rozděleny softwary na geografické informační systémy, systémy modelování a simulaci, systémy monitorovací, komunikační systémy, speciální databáze krizového řízení a další. Byl popsán vztah informací k těmto softwarům.

Článek stručně popsal metodiku COBIT a COBIT kostku a částečně ji aplikovala do oblasti softwarů krizového řízení. Pro tuto problematiku byly definovány zdroje, a formou příkladů byly nastíněny vazby a některé problémy.

K závěru je nutné opět podotknout, že tato oblast je komplexní, komplikovaná a dynamicky rostoucí a proto je potřeba ji neustále sledovat a hledat způsoby jak tuto oblast zlepšit.

Tento článek může soužit jako uvedení do dané problematiky a nastiňuje možný další vývoj, jenž může být mimo jiné i zvyšování bezpečnostního povědomí v otázkách informací v krizovém řízení, jak obecně tak i přímo v softwarech krizového řízení.

Literatura a informační zdroje

[1] ČESKÁ REPUBLIKA, Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti, 2005. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, ročník 2005, 143/2005, 412/2005.

[2] Citlivá informace, 2012. In: *KTD - Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha: ExLibris, NK ČR [cit. 2016-11-07]. Dostupné z: http://aleph.nkp.cz/publ/ktd/00000/03/000000388.htm

[3] DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ, 2008. *Řízení bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-86946-88-7.

[4] COBIT, 2014. *Iowa state university* [online]. Ames: Iowa State University of Science and Technology [cit. 2016-11-07]. Dostupné z: http://www.internalaudit.iastate.edu/internal-controls/cobit

[5] *COBIT 5 v malých a středních firmách, 2015. Systemonline [online]. Praha: CCB spol. s r.o. [cit. 2016-11-10]. Dostupné z: https://www.systemonline.cz/sprava-it/cobit-5-v-malych-a-strednich-firmach.htm*

[6] POŽÁR, Josef, 2005. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

[7] *Management of information security*, 5th edition. ISBN 978-130-5501-256.

[8] SMITH, Richard E., *Elementary information security*. Second edition. ISBN 12-840-5593-0.

[9] WHITMAN, Michael E. a Herbert J. MATTORD, *Principles of information security*. Fifth edition. ISBN 978-128-5448-367.

[10] DRASTICH, Martin, 2011. *Systém managementu bezpečnosti informací*. Praha: Grada. Průvodce (Grada). ISBN 978-80-247-4251-9.

[11] LIDINSKÝ, Vít, Ivana ŠVARCOVÁ, Petr BUDIŠ, Zbyněk LOEBL a Barbora PROCHÁZKOVÁ. EGovernment bezpečně. Praha: Grada. EAN 24763552.