POLITIKA BEZPEČNOSTI INFORMÁCIÍ V PODNIKU

Kister Łukasz *)

ABSTRAKT

Bezpečnosť informácií v podniku musí byť výsledkom holistickej stratégie ochrany všetkých procesov spracovania informačných aktív. Takáto stratégia musí brať do úvahy všetky doterajšie metódy spracovania dát, ako aj tie, ktoré budú dostupné v najbližšej budúcnosti.
Tento článok prezentuje autorský model vytvorenia komplexného dokumentu, ktorý definuje všetky elementy bezpečnosti informácií vo firme – Politiky bezpečnosti informácií.

Kľúčové slová:
Informácia, bezpečnosť, podnik, politika

ABSTRACT

Information security in the company should be based on the holistic strategy of the protection of all the processed information assets. Such a strategy must take into account all the current methods of data processing as well as those that will be available in the nearest future.
This article present the author's model of the construction of the comprehensive document defining all the elements of the information security of the company - Information Security Policy.

Key words:
Information, Security, Company, Policy

*) Łukasz Kister, Mgr. doktorand na Katedre bezpečnostného manažmentu Fakulty špeciálneho inžinierstva Žilinskej univerzity v Žiline, vedúci sekcie doktorandov European Association for Security, generálny riaditeľ Information Security Service, mobil: +48 880 147 767, e-mail: l.kister@bezpieczneinformacje.pl,

1 AKTUÁLNY STAV VÝSKUMU BEZPEČNOSTI INFORMÁCIÍ V PODNIKU

1.1 INFORMAČNÉ AKTÍVA PODNIKU

V Európskej únii sa za podnik považuje „*každý subjekt, ktorý vykonáva hospodársku činnosť bez ohľadu na jeho právnu formu. Sem patria najmä samostatne zárobkovo činné osoby a rodinné podniky, ktoré vykonávajú remeselnícke alebo iné činnosti a partnerstvá alebo združenia, ktoré pravidelne vykonávajú hospodársku činnosť.*“ [10].

Informačné aktíva[1] sú všetky nehmotné zdroje organizácie obsiahnuté v tradičnej dokumentácii, databázach, informačnom systéme a v hlavách osôb, ktoré ho tvoria.

Jeden zo všeobecných spôsobov členenia informačných zdrojov v podniku bol navrhnutý **Mariou Romanowskou**, ktorá vyčlenila dve skupiny pri zohľadnení nižšie uvedených charakteristických vlastností: formálne vlastnícke právo a možnosť skutočného finančného ocenenia (napr. patenty, licencie, databázy) alebo nemožnosť ocenenia (napr. vedomosti, zručnosti, kompetencie) [12, s. 28]. V literatúre sa stretneme aj s podrobnejším členením informačných aktív, ktoré rozlišujú nižšie uvedené prvky: forma, cieľ, zdroj pôvodu, význam alebo funkcie [11, s. 25-27].

V súčasnosti sa za kľúčovú skupinu nehmotných aktív hospodárskych organizácií považuje špecifický druh vedomostí, nazývaný anglickým pojmom „**know-how**“[2], ktorým sa označuje vedomosti: praktické, utajované, iným neznáme, vyplývajúce zo skúseností, ktoré majú slúžiť priamo na získanie hospodárskych výsledkov, a nie na všeobecné poznanie [7, s. 17]. Tento zdroj tvoria vedomosti formalizované v dokumentoch a databázach, ale aj v hlavách osôb, ktoré tvoria organizáciu, práve túto ich formu je najťažšie popísať a pritom má obyčajne najväčšiu hodnotu.

V prípade predmetu tejto práce sa zdá opodstatnené, aby sme prijali členenie zdrojov informácií pri zohľadnení všeobecného kritéria **úrovne dostupnosti**. Ako tvrdí **Wiesław Kotarba**, je to najvýstižnejšie členenie v prípade hospodárskej činnosti. Autor uvádza jeho tri stupne:

- **neverejné informácie (utajované)** – sú také, ktoré neboli zverejnené, a spôsob, ktorým je zabezpečený ich primeraný stupeň ochrany bol určený vo všeobecne platných predpisoch, v niektorých prípadoch v interných predpisoch alebo vyplýva z dvojstrannej občianskoprávnej zmluvy;
- **chránené verejné informácie** – sú také, ktoré sú sprístupnené, aby bolo možné sa s nimi zoznámiť, ale ich využitie na hospodárske účely je možné iba spôsobom a na zásadách určených právom, sú to napr.: vynálezy, úžitkové vzory, ochranné známky, obchodné značky, diela podliehajúce autorskému právu a pod.;

[1] Informačné aktíva – (angl.) Information Assets (Resources).
[2] Know how – vedieť ako.

- **úplne verejné informácie** – dostupné pre verejnosť (povinne alebo voliteľne) v rôznej forme, ku ktorým je potrebné priradiť aj informácie v minulosti utajované, pre ktoré z rôznych príčin vypršalo ochranné obdobie [7, s. 18-21].

1.2 RIADENIE BEZPEČNOSTI INFORMÁCIÍ

Pri analýze pojmov **informácie** a **bezpečnosti**, a následne pri ich syntéze (kompilácii) môžeme prísť k nasledujúcej definícii:
„***Bezpečnosť informácií je schopnosť kreatívnej informačnej aktivity subjektu a znamená určitý objektívny stav založený na absencii ohrození v oblasti vlastných informačných zdrojov subjektívne vnímaný jednotlivcami alebo skupinami, ktoré sú ich majiteľmi.***“

Na tomto základe budeme v súlade s definíciou **Ladislava Hofreitera** **bezpečnosť informácií** chápať, ako „*zachovanie prístupu k potrebným informačným zdrojom pri súčasnom zaručení ochrany tých vlastných informácií a zdrojov, u ktorých si to vyžaduje dôležitý záujem objektu (osoby, štátu, podniku ap.)*“ [3, s. 52].

V súlade s predchádzajúcimi konštatáciami **bezpečnosť informácií** je **dynamickou situáciou, ktorá smeruje k obmedzeniu pravdepodobnosti výskytu ohrození v oblasti chránených informačných zdrojov, ktorá zahŕňa ich všetky atribúty**.

V súčasnosti je praktická činnosť v oblasti bezpečnosti informácií stále častejšie nazývaná pojmom „**riadenie bezpečnosti informácií**“ a v takej forme tvorí najširší predmet výskumu.

Andrzej Białas ho definuje ako „*interdisciplinárnu oblasť na styku informatiky, práva, organizácie a riadenia, ktorá sa zaoberá definovaním, dosahovaním a udržiavaním bezpečnosti*“ [2, online].

Pri detailnejšom pohľade na subjekt bezpečnosti definovaný v slovníku pojmov pripravenom na **Fakulte špeciálneho inžinierstva Žilinskej univerzity**, za **riadenie bezpečnosti informácií** môžeme označiť: *špecifickú cieľavedomú činnosť zameranú na odvrátenie alebo minimalizáciu rizík alebo rôzneho druhu ohrození informačných zdrojov obsahujúcu v sebe prvky rizikového, krízového, havarijného a hodnotového manažmentu* [9, s. 20].

Preto pri zohľadnení **tradičnej definície riadenia** sú to: *profesionálne aktivity, založené na spoľahlivých vedomostiach, odborných zručnostiach, overených metódach, správnych a účinných spôsoboch a technikách konania, smerujúce k dosiahnutiu bezpečnosti informačných zdrojov subjektu.*

Pri zohľadnení hore uvedených atribútov **Tadeusz Kifner** za „**bezpečnú informáciu**“ považuje len takú, ktorá „*vďaka svojmu obsahu dokazuje, že je autentická, integrálna, dôverná, jej odoslanie je nepopierateľné a bola a je dostupná len pre osoby na to oprávnené*“ [4, s. 22].

V procese riadenia bezpečnosti informácií sa môžeme stretnúť s dodatočnou, podrobnou typológiou bezpečnosti. Podľa **Tomáša Lovečka** v oblasti bezpečnosti

informácií, ktorú označuje anglickou skratkou INFOSEC[3], môžeme vyčleniť nižšie uvedené typy bezpečnosti:

- **fyzická bezpečnosť** (PHYSEC[4]) týkajúca sa ohrození subaktív[5] nevyhnutných pre fungovanie informačného systému;
- **počítačová bezpečnosť** (COMPUSEC[6])– týkajúca sa fyzických ohrození subaktív počítačových systémov nevyhnutných pre spracovávanie informácií;
- **osobná bezpečnosť** (PERSEC[7]) – týkajúca sa ohrození informačných aktív vyplývajúcich z ľudského faktoru;
- **komunikačná bezpečnosť** (COMSEC[8]) – týkajúca sa ohrození informačných aktív počas ich spracovávania, uchovávania a prenosu;
- **logická bezpečnosť** (LOGISEC[9]) – týkajúca sa ohrození fungovania prvkov nevyhnutných pre riadenie prístupu k zdrojom informácií [8, s. 12-13].

Na záver musíme súhlasiť s názorom **Piotra Bączka**, ktorý v procese riadenia bezpečnosti informácií prikazuje zohľadniť: „*široký rozsah oblastí života, ktoré môžu generovať ohrozenia rôzneho druhu a ktoré sa vyznačujú vlastnou špecifickosťou a môžu osobitne ovplyvňovať informačné zdroje*“, ku ktorým okrem iného započítava oblasti: „*sociálnu, etickú, kultúrnu, vedeckú, hospodársku, politickú, vojenskú, oblasť medzinárodných vzťahov*“ [1, s. 75-76].

2 POLITIKA BEZPEČNOSTI INFORMÁCIÍ

2.1 POJEM

Politika bezpečnosti informácií je súbor zákonov, pravidiel a skúseností z praxe, ktoré regulujú spôsob riadenia, ochrany a distribúcie informačných zdrojov v rámci organizácie, týkajúcich sa celkovo problému ich zabezpečenia, či už sú spracúvané tradične alebo v informačných systémoch [5].

Jej cieľom je **vytvoriť a udržať pre organizáciu akceptovateľnú úroveň ochrany spracúvaných informačných zdrojov pred ohrozením,** a súčasne dodržiavať právne predpisy týkajúce sa bezpečnosti informácií, ktoré obsahujú rôzne dôverné dáta, napr. osobné údaje.

2.2 DOKUMENT POLITIKY BEZPEČNOSTI INFORMÁCIÍ V PODNIKU

[3] Angl. Information Security.
[4] Angl. Physical Security.
[5] Subaktíva – všetky prvky systému, ktoré slúžia na spracovávanie informácií, [8, s. 10].
[6] Angl. Computers Security.
[7] Angl. Personal Security.
[8] Angl. Communications Security.
[9] Angl. Logical Security.

Na základe praktickej implementácie celkových zásad bezpečnosti informácií v rôznych podnikoch autor vypracoval nižšie uvedený **model dokumentu Politiky bezpečnosti informácií,** ktorého cieľom je systémový opis prijatého štandardu ochrany informačných zdrojov.

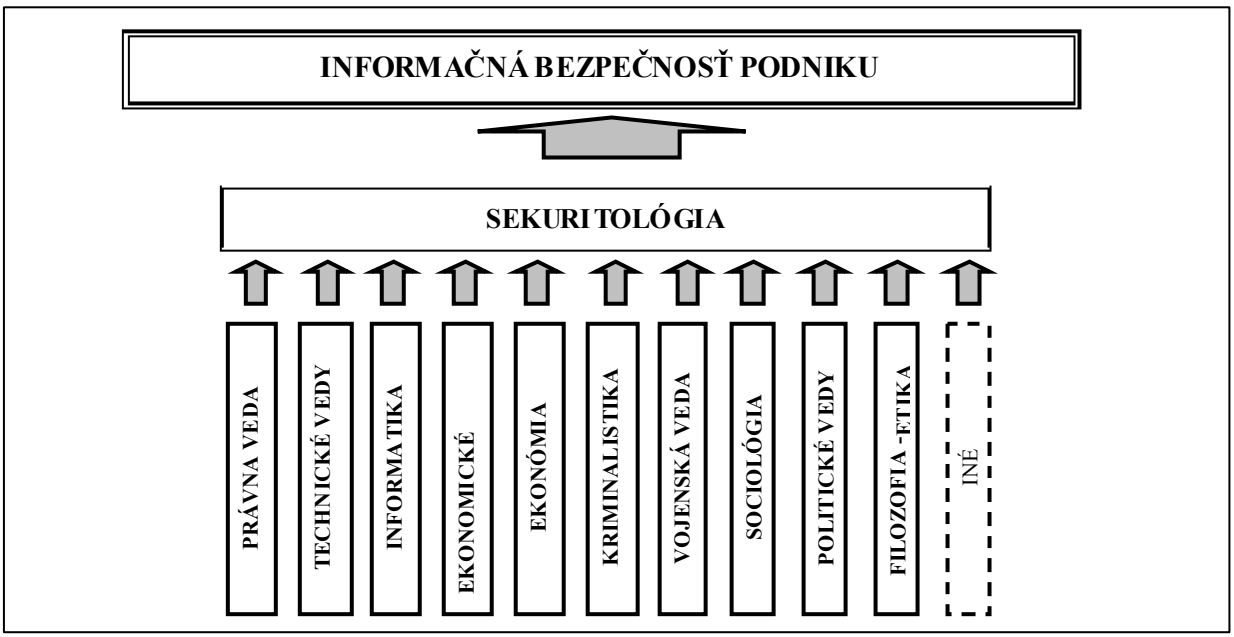
1. **Deklarácia vedenia** – je prvý dokument Politiky, povinná súčasť všetkých dokumentov spojených s procesom riadenia v organizácii. Predstavuje zámery vrcholového vedenia, ciele a zásady ochrany informačných zdrojov, a taktiež preukazuje bezprostredné zaangažovanie do tohto procesu. Hoci to tak nevyzerá, ma fundamentálny význam pre správne prijatie, realizáciu a fungovanie systému riadenia bezpečnosti.
2. **Všeobecné ustanovenia –** mali by definovať pojmy použité v rámci dokumentu, uviesť právny základ i cieľ, a stanoviť pravidlá používania.
3. **Organizácia riadenia spracovania informácií** – má určovať úlohy v procese riadenia, rozsah zodpovednosti a oprávnenia pomocou prehľadnej organizačnej tabuľky.
4. **Stratégia zabezpečenia informačných zdrojov –**mala by komplexne a prístupným spôsobom predstaviť technické a organizačné opatrenia prijaté organizáciou s cieľom zabezpečiť integritu, zodpovednosť a dôvernosť spracovaných informácií. V tejto časti by sa mali nachádzať záznamy týkajúce sa:
    - **osobnej bezpečnosti**;
    - **bezpečnostných zón – kontroly prístupu**;
    - **bezpečnosti tradičnej (papierovej) dokumentácie**;
    - **bezpečnosti technického vybavenia**;
    - **prístupu k informačnému systému**;
    - **prenosných počítačov a práce „na diaľku“**;
    - **dátových nosičov**;
    - **prístupu k verejnej sieti – Internet**;
    - **elektronickej pošty**;
    - **antivírusovej ochrany**;
    - **kryptografického zabezpečenia**;
    - **záložných kópií**;
    - **vyradenia technického vybavenia a dátových nosičov**;
    - **bezpečnostných auditov**;
    - **školení**;

    ako aj
    - **prístupu osôb „zvonku“ k osobným údajom.**
5. **Audit a aktualizácia dokumentácie** – táto časť prezentuje realizáciu aktivít, ktorými sa predchádza porušovaniu pravidiel prispôsobenia systémov bezpečnosti aktuálnej úrovni ohrozenia.
6. **Záverečné ustanovenia**

3 POTREBA VÝSKUMU BEZPEČNOSTI INFORMÁCIÍ

Informačná bezpečnosť podnikania sa ako predmet výskumu nachádza v okruhu záujmu rôznych vedeckých disciplín a ich predstaviteľov. Môžeme ich rozdeliť na tri skupiny podľa cieľov, metodológie, oblasti výskumu a výsledkov. Musíme tu uviesť také disciplíny ako právna veda, sociológia, technické vedy, ekonomické vedy, manažment, informatika, kriminalistika, politické vedy, ale aj policajné vedy, vojenská veda, ba dokonca i filozofia či telovýchova.

Uvedené disciplíny ale neberú do úvahy široké spektrum faktorov, ktoré môžu vytvárať rôzne druhy ohrození, a ktoré majú svoje vlastné špecifiká, čím môžu synergicky vplývať na informačné zdroje, keďže sa sústreďujú len na vlastnú oblasť výskumu. To bolo vlastne podstatou vzniku **sekuritológie**, vedy o bezpečnosti človeka a spoločenských útvarov. Vo svojom zameraní berie do úvahy rôznorodé faktory – objektívne i subjektívne, sociopsychologické i kultúrne, politické i právne, biologické i technické, makro- aj mikroekonomické, ktoré podmieňujú ohrozenia [3, 6, 13].



Obr. 5 Vedecká podpora informačnej bezpečnosti podniku
Zdroj: vlastné vypracovanie

Súčasný stav bezpečnosti, a hlavne informačnej bezpečnosti podniku jednoznačne potvrdzuje potrebu holistického pohľadu a úzkej spolupráce expertov i vedeckej obce v tejto oblasti. To je vlastne aj úlohou autora tohto článku.

LITERATÚRA

[1] BĄCZEK P.: Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Toruň: Wydawnictwo Adam Marszałek, 2006.

[2] BIAŁAS A.: *Zarządzanie bezpieczeństwem informacji*, [online], „NetWorld", 01.03.2001, [09.01.2011]. Dostupné na stránke: http://www.networld.pl/artykuly/8098_0/Zarzadzanie.bezpieczenstwem.informacji.html

[3] HOFREITER L.: *Securitológia*, Liptovský Mikuláš: AOS, 2006.

[4] KIFNER T.: *Polityka bezpieczeństwa i ochrony informacji*, Gliwice: Wydawnictwo Helion, 1999.

[5] KISTER Ł.: *Polityka Bezpieczeństwa Informacji – jako przykład realizacji prewencji kryminalnej na poziomie przedsiębiorstwa*, (w:) Prevencia kryminality na miestnej a regionalnej urovi, [CD-R], Žilina: Žilinská univerzita, 2009.

[6] KORZENIOWSKI L.F.: *Informačná bezpečnosť podnikania*, Žilina: Multiprint, 2010.

[7] KOTARBA W.: Zarządzanie wiedzą chronioną w przedsiębiorstwie, Varšava: ORGMASZ, 2001.

[8] LOVEČEK T.: Bezpečnostné systémy. Bezpečnosť informačných systémov, Žilina: EDIS, 2007.

[9] MIKOLAJ J., HOFREITER L., MACH V., MIHÓK J., SELINGER P.: *Terminológia bezpečnostného manažmentu. Výkladový slovník*, Košice: Multiprint, 2004.

[10] Odporúčanie Komisie č. 2003/361/ES zo 6. mája 2003 o definícii mikro, malých a stredných podnikov, oznámené pod dokumentačným číslom C (2003) 1422 (Ú.v. EÚ L 124)

[11] PIECZYKOLAN R.: *Informacja marketingowa*, Varšava: Polskie Wydawnictwo Ekonomiczne, 2005.

[12] ROMANOWSKA M.: Kształtowanie wartości firmy w oparciu o kapitał intelektualny, (v:) System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa, BOROWIECKI R., ROMANOWSKA M. (red.), Varšava: DIFIN, 2001.

[13] REITŠPIS J. a kol.: *Manažérstvo bezpečnostných rizík*, Žilina: EDIS, 2004.

Článok recenzoval:
Ing. Alexander Kelíšek, PhD.

CRISIS SITUATIONS SOLUTION IN SPECIFIC ENVIRONMENT

The 17th International Scientific Conference

30th – 31st May 2012

We would like to inform you that the Faculty of Special Engineering of the University of Zilina organizes an international scientific conference called **Crisis Situations Solution in Specific Environment**.

The goal of the conference is to exchange the latest findings and practical experience of crisis management, persons and property protection and the tasks of human factors in crises situations.

Conference sections:

Section No.1:	**General Principles of Crisis Management**
Section No.2:	**Security Management – People and Property Protection**
Section No.3:	**Solution of Risks and Crises in Economic Environment**
Section No.4:	**Human Factor in Crisis Management**
Section No.5:	**Fire Protection and Rescue Services**
Section No.6:	**Transport in Crisis Situations**

For further information please visit our web page **http://fsi.uniza.sk/kkm/** or contact our secretary of the conference on e-mail: **crisis@fsi.uniza.sk** or by phone: **+421 41 513 67 48**.

We are looking forward to meet you in Zilina

Faculty of Special Engineering, University of Zilina,
Ul.1.mája 32,
010 26 Zilina,
Slovak republic